02_hj32_edit 18-08-2003 9:55 Pagina 2

HACKER JOURNAL

Anno 2 - N. 32
28 Agosto - 11 Settembre 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it

Contributors: Bismark.it, Nicola D'Agostino, Devilman, 3do, Roberto "dec0der" Enea, Lele, Norloz, Robin, Angelo Rosiello, {RoSwElL}, Roberto (Whisper0fWind) Valloggia

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Copertina: Zocdesign.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

Gli articoli contenuti in Hacker Journal hanno uno scopo prettamente didattico e divulgativo. L'editore declina ogni responsabilita' circa l'uso improprio delle tecniche che vengono descritte al suo interno. L'invio di immagini ne autorizza implicitamente la pubblicazione gratuita su qualsiasi pubblicazione anche non della 4ever S.r.l.

Copyright 4ever S.r.l.
Testi, fotografie e disegni, pubblicazione anche parziale vietata.

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack'er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

FELICE ANNO NUOVO

Per il mondo occidentale l'anno inizia il 1 gennaio; il capodanno cinese si calcola con una formula piuttosto complicata (la prima luna nuova del nuovo anno solare, calcolato però tenendo conto di una sorta di "mese bisestile" che viene inserito dopo un certo numero di anni...). Per me, tuttavia, il periodo in cui faccio un bilancio dell'anno passato, e buoni propositi per quello che viene, è sempre stato attorno all'inizio di settembre. Sarà un po' un retaggio dei tempi della scuola (proprio in quei giorni iniziava un nuovo anno scolastico), o forse perché solo dopo un paio di settimane di vacanza riesco a tirare il fiato e fare progetti a medio termine, ma il mio capodanno personale coincide più o meno coi giorni in cui avrete tra le mani questo numero di HJ. Lo scorso anno HJ ha dimostrato una cosa importante: essere qualcosa di più di un fenomeno editoriale o una moda passeggera. HJ è qui per restare, nonostante le testate dedicate all'hacking si moltiplichino in edicola, e malgrado ogni mese le riviste di informatica "blasonate" e "tradizionali", strillino in copertina titoli che persino noi avremmo pudore a pubblicare (Copia i DVD, Scarica tutto da Internet, Sesso gratis in Rete...).
Il sito, che un anno fa era formato da qualche pagina statica con annunci relativi alle uscite della rivista, gli arretrati e poco più, ora è la "casa digitale" di una folta comunità di utenti, che interagiscono tra loro sul Forum e arricchiscono i contenuti del sito con articoli e notizie. Abbiamo anche aperto nuove sezioni e servizi che rendono più stretto il legame con la rivista: la Secret Zone, ora ospita, programmi, sorgenti e contenuti collegati agli articoli della rivista, ma che difficilmente possono trovare posto sulla carta. E grazie al nostro Free Internet abbiamo offerto a tutti la possibilità di collegarsi gratuitamente a Internet senza dover "vendere l'anima" a uno spammer.
Direi che le cose marciano bene, ma non vogliamo adagiarci sugli allori, e abbiamo in serbo parecchie novità per i prossimi mesi. Sicuramente torneremo a farci vedere in Smau, con i nostri soliti modi un po' dissacranti. E sicuramente continueremo a vigilare sui temi più scottanti che attraversano la rete: leggi liberticide e tasse-truffa, dialer sparati con la complicità delle compagnie telefoniche e spam istituzionalizzato. Aspettiamo però anche i vostri suggerimenti, i vostri commenti e le vostre critiche: di cosa volete che ci occupiamo? Quali argomenti dovremmo trattare? In che modo? Fatecelo sapere scrivendo a redazione@hackerjournal.it. Magari anche proponendovi per realizzare l'articolo (siamo sempre alla ricerca di nuovi collaboratori preparati e appassionati). Attendiamo i vostri messaggi.
Per ora, non mi resta che augurarvi, Felice Anno Nuovo!

grand@hackerjournal.it

LA NUOVA NEWSLETTER

I diecimila iscritti alla nostra newsletter lo sanno: il giorno che HJ viene distribuito in edicola, mandiamo un annuncio a tutti, con i principali argomenti trattati sulla rivista. Oltre a non perdere un argomento che sia uno, la newsletter permette anche di rimanere informati su tutte le attività collegate alla rivista: arretrati, collection, gadget, concorsi, novità sul sito.
A partire dallo scorso numero, la newsletter è disponibile in due "gusti": nel tradizionale formato solo testo o in Html, con grafica e link diretti al sito.

E' possibile iscriversi gratuitamente, cancellarsi o cambiare il formato predefinto (testo o html) dalla pagina che trovate all'indirizzo www.hackerjournal.it/php-bin/newsletter, o seguendo il link che trovate in home page.

Free Internet

Dal mese di luglio è attivo il servizio di collegamento a Internet targato Hacker Journal: indirizzo email @hackerjournal.it con 5 Mbyte, accesso super veloce fino a 128 Kbit al secondo (ISDN multilink PPP), server newsgroup, controllo anti virus e anti spam. Corri subito a iscriverti all'indirizzo www.hackerjournal.it/freeinternet.

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: 7mbre
pass: compl8

HACKER JOURNAL

STAMPA LIBERA NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

mailto:
redazione@hackerjournal.it

UNO SPORCO LAVORO...

Sono decisamente un newbie (uno dei primissimi abbonati alla vostra rivista) con poche nozioni di hacking. Non vi invento storielle che tanto non ci credereste, quindi vi dico esattamente le cose come stanno. Su un PC con Win2K con SP4 sono configurato come utente con restrizioni ma ho bisogno di crackare la pwd dell'Amministratore.
Vi spiego. Chi è stato investito dell'amministrazione della rete non è proprio una persona preparata in materia di PC ma ha pensato bene di impostare questa configurazione per dimostrare che comanda lui (nazista) tra l'altro il suo ufficio non è neanche qui. Morale quando ho dei problemi oppure ho la necessità di installare sul PC qualcosa che mi serve anche solo per il mio lavoro sono bloccato. Ho downloadato pwdump2, L0phtcrack 2.5 ed anche John The Ripper. Ma seguendo anche le istruzioni di un tutorial non riesco ad avviare pwdump2 dal prompt dei comandi. Mi esce la scritta: "Failed to open lsass: 5. Exiting."
Mi date qualche consiglio o dritta su dove altro posso rivolgermi?

Seraff

Aggirare la protezione non è una buona idea. In primo luogo, potresti essere sanzionato dalla tua azienda, o peggio ancora querelato per la manomissione del sistema. In secondo luogo, non faresti altro che mettere una toppa a un meccanismo che evidentemente non funziona, nascondendo il problema ai responsabili. Invece, la prossima volta che ti chiedono di consegnare un lavoro urgente e importante, spiega a chi di dovere che non puoi farlo, perché l'amministratore ha impostato delle policy inadeguate. Scommettiamo che il problema si risolve?

☺ Tech Humor ☺

NUMERI PRIVATI

Di recente ricevo chiamate e squilli con numero privato a casa; la cosa comincia a darmi fastidio come posso sapere chi c'è dietro al numero privato? Con il servizio 400 di Telecom Italia non funziona, però in cuor mio so che un modo ci sarà (magari grazie al PC).

Angelus

Il modo esiste, ma è meglio se lasci stare il PC e ti rivolgi alla PS. Per conoscere un numero riservato devi infatti sporgere denuncia alla Polizia o ai Carabinieri, e lasciare che siano loro a fare le indagini.

PIRATERIA/1

Ho letto il vostro articolo sulla pirateria del numero 30: l'articolo è interessante e veritiero sotto molti aspetti, però, come spesso succede la verità non è mai da una parte sola: si potrebbe per esempio dire che Autocad, Windows, Office, e la Playstation (i tre nomi presi maggiormente di mira nell'articolo) sono tra i pochi che consentono ad esempio di effettuare copie di backup, e che semmai bisognerebbe prendersela di più con chi non consente questo diritto (sancito dalla legge come voi avete giustamente detto più volte). Per quanto riguarda la pirateria, questa viene combattuta (secondo me giustamente) in aziende e simili, non mi risulta che siano stati perseguiti privati cittadini, a parte forse chi distribuisce copie in quantità industriale. Ho l'impressione che il copyright sia come un vestito a taglia unica, o prendi quello o non lo prendi.

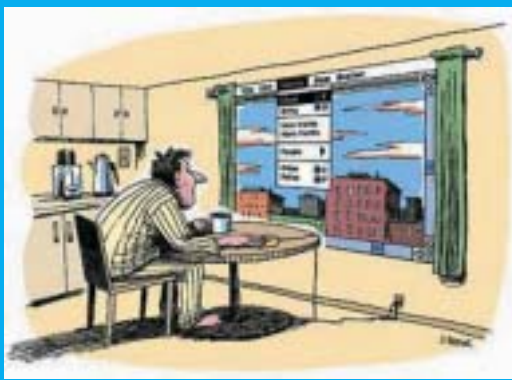
Paolo

☺ Tech Humor ☺

Bill Gates' daughter Jennifer visits Santa Claus

PIRATERIA/2

Ho letto il vostro articolo "Pirateria i conti non tornano" e devo ammettere che avete scritto quello che, spero e credo, tutti sanno!
Ma mi tocca fare una piccola piccola precisazione… devo mio malgrado spezzare una lancia a favore dell'Autodesk.
Mi spiego, nel vostro articolo, non avete neppure accennato a due non troppo piccole cose:
1) Avete giustamente detto che l'AutoCad è il programma di disegno TECNICO più diffuso (guardate che però AllPlan non se la passa male, almeno tra gli arch.!!) e che NOI (sono studente di ing. Edile-Architettura presso il Poli di MI) siamo fondamentalmente obbligati ad utilizzare i prodotto Autodesk ma NON avete detto che basta fare uno zapping tra le pagine del sito dell'Autodesk per imbattersi in promozioni (sorprendenti) per studenti: a 100 € + o – l'AutoCad 2004 …. (http://estore.autodesk.com/dr/v2/ec_MAIN.Entry10?V1=317009&PN=1&SP=10023&xid=25831&DSP=&CUR=978&PGRP=0&CACHE_ID=0)
2) Non avete detto neppure detto che basta rivolgersi alla ProgeSOFT per avere un IntelliCAD (http://www.progesoft.com/compra/index.asp?left=archt) a 200-300 € + o -, - se vogliamo prendere il pacchetto completo! - che guarda caso gira su un motore ACAD (che come dice la parola stessa è quello che fa funzionare l'AutoCad); inutile dire che è compatibile praticamente al 100% e che

03_05_hj32_posta 18-08-2003 9:56 Pagina 5

l'Autodesk ha fatto una ca**ata a firmare il contratto (che io definisco suicida –visto quello che poi fa-) che la obbliga a fornire alla ProgeSOFT tutti i motori ACAD, ma proprio tutti... vuol dire che se le cose non cambiano fra 10 anni avrà il motore aggiornato.
Come vedete non è obbligatorio sputar fuori 5.000 € per fare l'Università o per aprire un attività restando "compatibili e lobotomizzati".

Aner

HACKING LICENCE
1. zK8@3kSq
2. ***********
3. xx/xx/xx nowhere
4a. &&/&&/&& 4b. &&/&&/&& 4c. HKLA
5. FDKZZY83TF689QWKKO 34
7.
8.** KERBEROS COURT, ANONYMOUS ROAD INVISIBLE CITY - NOWHERE
9. A,B,B1,f,k,p

Vi mando l'immagine della mia patente opportunamente ritoccata per Hackerjournal, credo che esprima bene il concetto di anonimato!

ZeNitH

IN RISPOSTA A LUCA C./1

La mail di Luca mi lascia di stucco.
Invece di criticare una legge palesemente ingiusta, se la prende con il tizio che si è scaricato qualche mp3 col P2P. Ma soprattutto dichiara di non aver mai scaricato mp3 e ritiene che lui debba pagare per le malefatte altrui.
Buongiorno ben svegliato eccoti nella tua desertica realtà. La tua logica fa acqua da tutte le parti. Seguendo il filo del tuo ragionamento si dovrebbe andare al ristorante con gli esami del sangue.
"Cosa desiderate x dolce. Ahi ahi ahi... cosa vedo colesterolo troppo alto mi spiace x il signore niente" Xchè tu sai quanto ci costa tutto sta gente che si ingozza e poi gli piglia un bell'infarto??
Non parliamo di chi fuma, chi guida troppo velocemente, chi sta a casa malato anche quando è sano, sesso senza protezione ecc. Il limite fra un regime totalitario e una democrazia è molto labile.
Al cittadino deve essere concesso anche il lusso di sbagliare, è il minimo x essere persone libere. La società civile offre anche indubbi vantaggi, cmq se non ti va puoi sempre accamparti in montagna (senza lettore mp3).
La legge è al servizio delle persone e non viceversa.
Se la maggioranza delle persone sente la necessità di condividere con gli altri allora la legge si dovrà adeguare, non è possibile che x l'avarizia di pochi debbano pagare in molti.
Eppoi sei così sicuro che senza furti i prezzi scenderebbero?
Chi si scarica un CD da Internet difficilmente lo comprerebbe non avendo alternative, ma dopo averlo visionato è + probabile un potenziale acquisto.
Le case discografiche non ci perdono anzi semmai si fanno un sacco di pubblicità gratis.
Per concludere poi ti dico che il paragone sulla casa e assai ridicolo.
Non vorrai paragonare un file con un oggetto fisico?
Mettetevelo bene in testa questo è un altro mondo. Posso fare 1000 copie di un mp3 e ognuna sarà uguale in tutto e per tutto all'originale. Non è come un piatto di pasta che o la mangio io o la mangi tu.

Giaipur

Non sono pienamente d'accordo. Chi si comporta male deve essere sanzionato; quello che è sbagliato è penalizzare tutti per punire qualcuno.

IN RISPOSTA A LUCA C./2

Nella rubrica mailto: del numero 30 di hj non mi è piaciuta la vs risposta ad una email intitolata "due articoli di giornale" di luca C.
Premesso che compro regolarmente hj sin dal primo numero e che condivido in pieno il contenuto della email di Luca, trovo la vs risposta fuori luogo.
Parlate di etica-hacker, di hacker vs cracker, etc... e non potete, a mio avviso naturalmente, dare una risposta che potrebbe passare per "ammiccante" nei confronti di certe situazioni.
Se vogliamo veramente far in modo che il termine hacker rappresenti "...gli onnivori della conoscenza ... i pionieri delle nuove frontiere tecnologiche ..." (tratto liberamente dal numero 30 di hj) si deve prendere anche una posizione netta verso certi comportamenti
Confido in una risposta con la r maiuscola, non tanto alla mia email ma quanto a quella di Luca.

ddd

Come dicevo sopra, il punto della questione è che non si può restringere le libertà di tutti, o imporre tasse a tutti, per punire il comportamento scorretto di qualcuno. A nessuno viene in mente di imporre una tassa sul conto corrente per compensare le banche rapinate, né tanto meno di tassare la vendita di armi per risarcire le vittime di armi da fuoco (questa sì che ci vorrebbe...). Se si fanno leggi scellerate che colpiscono tutti e che sanno di rappresaglia, bisogna prendersela col legislatore, che dovrebbe fare in modo di punire il singolo che sbaglia, e non una massa indistinta.

Gentili amici di Hacker Journal, volevo segnalarvi che l'URL del mio sito è stato confuso con un altro. Nella sezione programmazione, il link del mio sito "Killme In The Net", non è esatto, infatti cliccandoci sopra si accede al sito Spaghetti Hacker. L'URL giusto è **http://www.killmeinthenet.3000.it**

NEWS

NUMERI

PISTOIA SCEGLIE L'OPEN SOURCE

Il Consiglio Comunale di Pistoia ha dato la sua approvazione a una mozione che propone la scelta del software libero come alternativa prioritaria rispetto al software proprietario quando si viene alla definizione dei sistemi informativi della pubblica amministrazione. La mozione chiede anche che vengano attivati per il personale del Comune di Pistoia corsi di aggiornamento per l'uso del sistema operativo Linux e che siano resi operativi contatti con gruppi ed associazioni locali che possano contribuire alla diffusione del software libero sul territorio, nelle scuole e presso tutti i cittadini.

UN GUANTO PER PARLARE

Jose Hernandez-Rebollar, un ricercatore americano, ha inventato l'AcceleGlove, un guanto del tipo di quelli usati nelle applicazioni di realtà virtuale, in grado di tradurre in testo o parole il linguaggio dei segni utilizzato dai sordomuti. Progetti analoghi erano già stati messi a punto anche in campo militare, per consentire ai soldati di comunicare tra loro in modo silenzioso, ma in questo caso si tratta di un linguaggio piuttosto semplice, e numericamente limitato.

L'AcceleGlove, dotato di un wearable computer, potrà invece interpretare anche i movimenti più complessi ed impercettibili della mano e del braccio, e convertirli in parole e frasi.

Secondo uno studio, solo negli Stati Uniti le persone prive di udito sono circa 28 milioni, e il suo inventore assicura che questo guanto permetterà loro di dialogare quotidianamente con chi non conosce il linguaggio dei segni.

ARRIVA IL DIGITALE TERRESTRE

E' stata l'emittente televisiva La7 la prima a sperimentare il digitale terrestre, il nuovo sistema di trasmissione che entro il 2006 dovrebbe sostituire quello analogico. La sperimentazione commerciale del dtt per La7 è iniziata a giugno in cinque aree geografiche da Torino a Bologna. Il test coinvolgerà un campione di più di 2.000 famiglie a cui se ne aggiungeranno altre 2.000 entro la fine dell'anno. Dal canto suo, Mediaset consegnerà subito dopo l'estate i nuovi decoder a un campione di 2.000 famiglie residenti lungo l'asse Nord-Ovest di Milano, fino a Varese. L'azienda intende coprire entro l'anno con due multiplex oltre il 50% della popolazione italiana. Anche la Rai ha approvato l'accordo di programma con il Ministero delle telecomunicazioni sul digitale terrestre. A differenza di Mediaset e Rai, La7 punterà sull'integrazione tra la nuova rete di TV digitale e quelle fisse e mobili di telecomunicazione.

SATELLITI PER I GORILLA

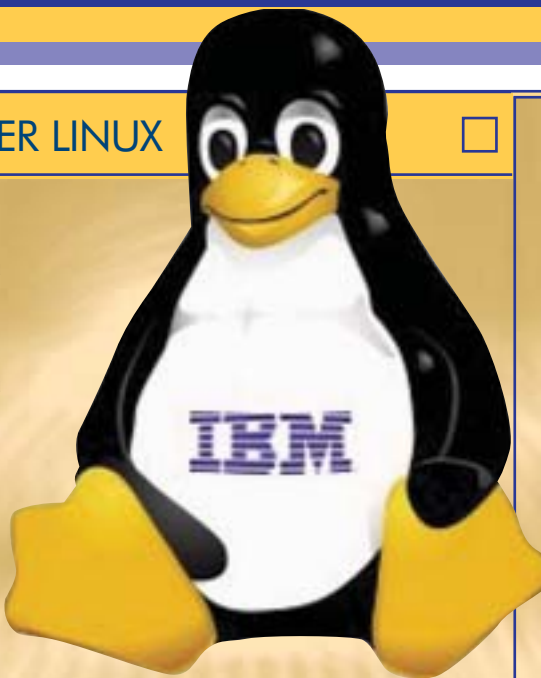
I gorilla di montagna sono una delle specie più a rischio del mondo. Per cercare di risolvere questo problema, l'Unesco utilizza i satelliti dell'Esa, l'Agenzia spaziale europea, per monitorare, fra le altre cose (i satelliti vengono destinati al monitoraggio di oltre 730 siti di patrimonio culturale o naturale nel mondo), anche i parchi nazionali africani in cui vivono, appunto, i gorilla. Gli insediamenti umani, la ricerca di combustibili, il virus Ebola, il bracconaggio e la cattura dei cuccioli per il commercio illegale, sono fra le cause principali che minacciano la sopravvivenza dei gorilla. Il progetto BeGo (Built Environment for Gorilla) di Esa e Unesco prevede la produzione di una serie di mappe dei parchi nazionali che si trovano nelle aree montagnose inaccessibili di Uganda, Ruanda e Repubblica Democratica del Congo, dove si trovano gli ecosistemi dei gorilla di montagna. I satelliti di osservazione civile della terra sono in grado di individuare dettagli di 60 cm e sono quindi ideali per registrare le modifiche nell'utilizzo del suolo. Tramite questo nuovo progetto si studieranno quindi le immagini satellitari per capire i cambiamenti dell'habitat dei gorilla.

È ORA DI GIOCARE

Liberi di pensare, liberi di giocare è il motto della nuova rivista di giochi per PC che si trova in edicola da ferragosto. Videogames Journal, questo è il suo nome, ha un prezzo scandalosamente basso: si trova a 3 € con CD e a 1,49 € senza CD, versione economica per chi ha già il computer pieno di demo e si scarica quel che vuole con l'ADSL o con la fibra ottica. Per di più ha uno stile completamente diverso dal solito, sta comodamente in qualsiasi borsa e, non ultimo, la fanno nella redazione accanto a quella di Hacker Journal, non racconta balle a nessuno e ci trovate solo roba genuina. Per scrivere alla redazione: **vj@videogamesjournal.it**

NEWS

IBM PUNTA SU POWER LINUX

IBM ha moltiplicato gli investimenti su Linux e in particolare quelli relativi al progetto per l'ottimizzazione di Linux per la piattaforma Power, la stessa con cui IBM vuol aggredire il mercato a 64 bit. IBM ha aumentato lo staff di sviluppatori che lavorano presso il proprio Linux Technology Center portandoli da 250 a 300. Fra gli obiettivi più immediati c'è il miglioramento del supporto all'hardware e ai sistemi di storage, l'implementazione dei servizi di gestione e delle funzionalità enterprise come l'SMP (symmetrical multiprocessor). Fra la linea di CPU Power c'è anche il giovane PowerPC 970, lo stesso processore utilizzato da Apple sui nuovi modelli di Power Mac G5 e da IBM su alcuni server blade.

ENERGIA DALL'UVA

Oltre che a produrre il nettare degli dei meglio noto come vino, l'uva è in grado di fornire niente meno che energia elettrica. Questo è quanto sostengono i ricercatori dell'università di Austin, Texas, che hanno messo a punto una cella biocombustibile. La cella, che sfrutta il metabolismo del glucosio e dell'ossigeno, non è per nulla costosa e potrebbe essere impiegata per alimentare una lampadina, per misurare la variazione di temperatura corporea indice di infezioni e molto altro ancora. Per adesso una cella ha una vita media di alcune ore. Con opportune modifiche potrebbe durare anche una settimana.

MOZILLA DIVENTA NON PROFIT

Mozilla.org (www.mozilla.org) diventa fondazione non profit. America Online nei prossimi due anni ha promesso un finanziamento di almeno due milioni di dollari per sostenere l'iniziativa. Ma la Mozilla Foundation potrà contare anche su altri supporti, visto il ruolo di sempre maggiore rilievo assunto dai suoi software per Internet. La Foundation promuoverà la distribuzione e l'adozione delle più importanti applicazioni basate sul codice di Mozilla, oltre a coordinare e incoraggiare lo sviluppo e il testing del codice di Mozilla. Fra i finanziatori della Mozilla Foundation compaiono anche IBM, Sun, Red Hat e Mitch Kapor, a suo tempo fondatore di Lotus e di del foglio di calcolo "Lotus 1-2-3". Kapor, che all'interno della fondazione ricoprirà la carica di chairman, ha messo a disposizione della nuova organizzazione una somma pari a 300mila dollari.

HOT!

ELETTORI PIGRI

Chi sperava che la comodità offerta dal voto elettronico potesse risvegliare le sonnacchiose coscienze politiche degli elettori, si sbagliava di grosso. In Inghilterra la sperimentazione delle urne elettroniche è stata un vero fallimento. Non solo si è registrato meno afflusso rispetto alle tradizionali, ma si sono anche verificati problemi di sicurezza e con essi tante perplessità.

C'É SPAM E SPAM

La Hormel, società produttrice della storica carne in scatola SPAM, che in passato aveva dichiarato di accettare l'uso del termine spam come emblema della posta-spazzatura, ha perso la pazienza, ed ha deciso di denunciare chi usa l'immagine delle proprie confezioni alimentari per promuovere determinati servizi antispam. Come molti ricorderanno, il termine spam indica qualcosa che si cerca di rifilare a forza a qualcuno, da quando il gruppo comico britannico Monty Python inscenò una storica ed esilarante gag (il video si trova anche su Internet: http://www.detritus.org/spam/skit.html), nella quale il cameriere di un ristorante, rimasto senza cuoco, cercava in mille modi di rifilare ai clienti la SPAM, la carne in scatola, come ultima risorsa.

Nel mirino di Hormel, che detiene il trademark Spam, figura in prima linea SpamArrest, che ha rifiutato di togliere il termine Spam dal proprio nome, ed ha di recente richiesto di registrare la propria ragione sociale come trademark a sua volta. La Hormel ha dedicato un'intera pagina del proprio sito (http://www.hormel.com/home.asp) alla spinosa questione, per chiarire che non intende concedere nulla alla realizzazione di prodotti dal nome Spam, in quanto termine "protetto".

siti; scegliete voi se tirarvela o vergognarvi

http://overnetcrew.altervista.org

Ciao belli! volevo chiedervi di linkare il sito della mia crew: GRAZIE

—=(HyTk0k)=—

www.hacksworld.tk

Vorrei poter vedere il mio sito segnalato sulla Vostra rivista.

Lord Menfi

http://brc.altervista.org

Ciao a tutti... ovviamente sono un vostro assiduo lettore e vi scrivo per segnalarvi il mio sito Internet. È ancora giovane e non tutte le sezioni sono attive, ma cresce rapidamente.

BrC

I classici della Rete

http://daemoncacum.cjb.net

Cara redazione vogliate pubblicare gentilmente il mio fantastico sito Web? Grazie infinite!

Daemoncacum

www.hackitalia.tk

Ciao a tutta la redazione di HJ vorrei segnalarvi il mio sito che secondo me è molto utile e pieno di informazioni e programmi interessanti.

Lordkrishna

http://www.fuckinworld.org

È un ottimo sito sull'hacking, forse il migliore in circolazione(dopo il vostro).
Saluti,
VOSTRO FAN

10_12_hj32_max 18-08-2003 10:01 Pagina 10

Zilog inside

MSX 20 anni di

Quest'anno si festeggia il ventennale dell'MSX, un home computer per molti versi rivoluzionario che a tutt'oggi conta numerosi estimatori e utilizzatori, e continua a stupire con nuovi progetti amatoriali e non.

La nascita ufficiale dell'MSX reca la data del **27 giugno 1983:** quando furono annunciate le specifiche dell'MSX1, base di quella che doveva essere la prima implementazione di un nuovo standard di computer nel settore home computing, **su imitazione di quanto accadde con il VHS nel campo dell'home video.**

>> La nascita dell'MSX

L'idea di base fu il prodotto della ASCII, un'impresa fondata dal pioniere dell'informatica giapponese (e non solo) Kazuhiro "Kay" Nishi, con la partecipazione della Microsoft. All'epoca Gates era fortemente legato a Nishi e **la ditta di Redmond fornì sia il sistema operativo che una versione apposita del suo Basic**, chiamati rispettivamente MSX-Dos e MSX-Basic.
Dietro alla ASCII c'era il supporto di **numerosi giganti dell'elettronica giapponese e mondiale**. A partire dall'autunno dell'83 furono prodotti computer MSX da numerosissime ditte: Canon, Casio, Fujitsu, Hitachi, JVC, Mitsubishi, NTT, Panasonic, Pioneer, Philips, Samsung, Sanyo, Schneider, Seikosha, Sharp, Sony, Toshiba, Yamaha, Yashica, solo per nominare le più famose (la lista completa è all'url www.faq.msxnet.org/hardware.html).
Ogni macchina, di base, rispettava i dettami delle specifiche dello standard, anche se ai costruttori veniva lasciata un'ampia libertà nella scelta di **potenziare le proprie macchine con caratteristiche aggiuntive**, che avrebbero potuto distinguerle da quelle della concorrenza, come fece ad esempio la Yamaha, che propose l'MSX come workstation musicale.

>> Qualche dato tecnico

Dal punto di vista hardware generale, l'MSX rappresenta un **ibrido fra una console per videogame ed una generica macchina CP/M-80** e, anche se nel corso degli anni seguenti la piattaforma ha avuto numerose evoluzioni (MSX2, MSX2+, MSX TurboR e derivati), le coordinate tecniche di base sono rimaste immutate.
È interessante notare che per progettare i computer MSX è stato usato come punto di partenza l'home computer Spectravideo SVI-318, a cui sono state ampliate alcune caratteristiche hardware e aggiunti nuovi comandi al linguaggio Basic. La parentela fra le due macchine è molto stretta: la prova è nel fatto che per lo Spectravideo era disponibile un emulatore in grado di far girare i programmi per MSX.
L'MSX, come molti altri computer degli anni '80 (ad esempio lo ZX Spectrum della Sinclair), **è a 8 bit ed è basato sul processore Zilog Z80**, che inizialmente lavorava a 3,58 MHz.
Questa frequenza è stata raddoppiata in alcuni modelli della terza generazione (MSX2+) e definitivamente nei mo-

i Zilog Inside

delli della quarta generazione (MSX Turbo R).
Il sistema video e quello audio sono gestiti da processori specifici, usati anche su altri computer: nell'MSX1 il chip per l'audio è lo stesso usato anche nel Texas Instruments TI-99/4, e nelle console ColecoVision e Coleco Adam, mentre l'audio è gestito dal processore AY-3-8910 della General Instruments, lo stesso usato dallo Spectrum128 e in alcune schede audio per PC.
Lo standard MSX prevede un minimo di 8Kb di memoria RAM, 16Kb di memoria ROM ed almeno uno slot per l'inserimento di cartucce software e/o interfacce per l'estensione del sistema con nuove periferiche. Nonostante la comparsa dopo solo due anni di floppy drive, **gli slot furono ampiamente usati per espansioni, sia hardware che software.**

>> Non solo in Giappone

Un esempio molto particolare di questo genere è la cartridge con il Sacro Corano, prodotta per le versioni arabe dell'MSX.
Infatti, anche se l'MSX **raggiunse il massimo della popolarità nel suo paese natale, il Giappone,** riscosse un buon successo anche in Corea, Europa (grazie alla Phillips ma non solo), Sud America, e fu diffuso anche in posti apparentemente insospettabili quali Unione Sovietica (fu usato nelle scuole e addirittura nelle missioni spaziali) e Paesi Arabi, mentre è praticamente ignoto negli USA.
Sono stati proprio gli utenti e gli appassionati nel mondo, che negli ultimi dieci anni hanno permesso all'MSX di resistere e anzi di stupire con incredibili hack e aggiunte prima che nella madre patria si muovesse di nuovo qualcosa a livello ufficiale. Ma di questo e di altro parliamo con **Enrico Barbisan** (http://space.tin.it/computer/enribarb), retrocomputerista ed esperto di MSX nostrano, nell'intevista che trovate nel riquadro.

Nicola D'Agostino
dagostino@nezmar.com

Kay Nishi: il papà dell'MSX

L'idea di un computer basato su uno standard è frutto della mente del dottor Kazuhiro Nishi, uno degli artefici del personal computing giapponese.
Nishi nella sua carriera è stato editore, fondando la ASCII e pubblicando la prima rivista di informatica nipponica nel 1977, traduttore (sue le versioni in Nihongo di "The Road Ahead" di Gates e "Being Digital" di Nicholas Negroponte), progettista per la Mitsubishi, amico e collaboratore di Bill Gates (che ha coinvolto nel progetto MSX), progettista nel team Microsoft che realizzò l'MS-DOS (e c'è chi afferma che Nishi fu cruciale nel convincere gates ad accettare la proposta di realizzare un sistema operativo per la IBM), oltre che ovviamente responsabile delle attività della ditta di Redmond nel paese del sol levante.
Insomma, una carismatica e bizzarra figura che ha creduto ed investito nell'MSX (e responsabile del recente revival della macchina), arrivando a pazzesche trovate pubblicitarie come un gigantesco dinosauro all'uscita della metropolitana di Tokyo, cosa che, per la cronaca, non piacque molto a Gates, il cui supporto alla causa dell'MSX scemò sensibilmente nella seconda metà degli anni '80.

INTERVISTA A ENRICO BARBISAN

Hacker Journal: **Com'è la situazione dell'MSX nel mondo?**

Enrico Barbisan: L'interesse attorno al sistema MSX non è mai scemato. Pur essendoci stati dei periodi di difficoltà, dovuti alla fine dello standard agli inizi degli anni 90, gli appassionati hanno sempre prodotto hardware e software di qualità in modo del tutto indipendente, ma ispirandosi comunque alla filosofia del progetto.
Un esempio sono le periferiche: espansioni di slot, cartucce megaram, kit 7 Mhz, le nuove RS-232, lettori di memorie Flash, e anche un'interfaccia IDE per il collegamento di CD-ROM, HD e Zip, che trasformano l'MSX in un vero sistema multimediale!

HJ: **Puoi fornire una stima degli utenti attuali?**

EB: Difficile: possiamo solo dire che siamo a migliaia e, soprattutto, molto motivati! A molti MSXiani va stretto il fatto di essere etichettati come retrocomputeristi, l'MSX è ancora una realtà viva e vegeta!

HJ: **E in Italia?**

EB: Il fronte italiano ricalca più o meno la situazione internazionale, con club e comunità online, anche se è molto interessante il fatto che gli italiani tendano a sostenersi con le sole proprie forze. Inoltre esistono anche utenti che in modo indipendente continuano a produrre applicazioni e videogame o si cimentano in progetti geniali come l'installazione di reti di home computer o connessioni di periferiche di ogni tipo. L'importante è che tutte queste iniziative non restino dei progetti isolati: molto importanti sono perciò gli incontri nazionali in tema MSX: visti i successi dei precedenti a Brescia e Spresiano (TV), si bisserà sicuramente anche quest'anno.

HJ: **Cosa succede in Giappone? Qual'è la tua opinione sulle recenti iniziative e sul futuro dell'MSX?**

EB: In Giappone l'MSX è ripartito alla grande! Nishi ha fondato l'MSX Association, che ora detiene i diritti del marchio MSX ed ha prodotto MSX-PLAYer, l'emulatore ufficiale dei sistemi MSX, che però al momento non può essere esportato al di fuori dei confini del Giappone perché la Microsoft, detentrice dei diritti del BIOS, non ne ha concesso l'esportazione. L'emulatore permetterà anche di giocare direttamente su PC con tutte le cartucce ROM originali MSX, grazie all'USB Cartridge Reader, uno slot MSX che si connetterà alla porta USB del PC.
Inoltre, in collaborazione con la ASCII, è stato pubblicato l'MSX Magazine, una rivista che solo in Giappone ha venduto più di 30.000 copie!
Un altro progetto giunto ormai a buon punto è il OneChip MSX, cioè l'integrazione in un unico chip di tutte le specifiche audio e video dell'MSX. Lo scopo sarebbe quello di fornire servizi multimediali e, integrato in dispositivi mobili, di reperirli direttamente da reti wireless, supportati dall'MSX-PLAYer che costituisce una sorta di "processore virtuale".
Per il futuro, infine, gli utenti si aspettano anche una nuova piattaforma MSX3, e per il momento girano voci di un OneChip affiancato da uno Z80 a 100 Mhz…
Gli utenti hanno accettato positivamente queste iniziative: forse è una strada buona per rivitalizzare queste "vecchie" tecnologie che danno ancora molte soddisfazioni, in barba agli sprechi di risorse cui l'informatica moderna ci ha ormai abituati.

MSX: PINGUINO INSIDE?

Una curiosità dell'MSX è il frequente uso del pinguino (http://www.msxnet.org/mess/mess-msx.png) come suo simbolo, anche di recente (http://www.zdnet.co.jp/news/0210/22/msx_01.jpg), scelta che condivide con il sistema operativo GNU/Linux. Il motivo della scelta di questo animale non è stato ufficialmente chiarito ma è probabilmente a causa di Penguin Adventure (ftp://ftp.funet.fi/ pub/msx/graphics/jpg/gamecovers/Penguin_Adventure_-Konami-.jpg), uno dei primi e più popolari giochi per MSX sviluppato dalla Konami.

Il BROWSER full-optional

Touchnet Browser ha tutto quello che si può desiderare ma non è gratuito.

In un numero precedente di HackerJournal si è detto che l'assoluto anonimato in Internet è praticamente impossibile per come è costruita la rete: l'unica soluzione per non farsi rintracciare è quella di far rimbalzare la nostra connessione attraverso dei server proxy. Questa operazione può risultare noiosa e lunga: alternative sono usare dei programmi come Multiproxy (freeware) o Anonymous 4 Proxy o scriversene uno, seguendo un po' le istruzioni presenti sempre su HackerJournal. Tutti questi programmi però richiedono l'uso di risorse ed inoltre bisogna configurare il proprio browser per usarli. In nostro soccorso arriva un browser sviluppato appositamente per avere una maggiore sicurezza in rete, e non solo. Si tratta di Touchnet Browser, un programma shareware reperibile presso www.touchingsoft.com al prezzo di 29,95 dollari, che si integra col motore di Internet Explorer aggiungendo alcune possibilità e permettendo un maggiore controllo sulla nostra navigazione.

Ogni pagina può essere smembrata e analizzata in ogni dettaglio.

>> Anonimità automatica

Questo programma offre diverse opzioni: la possibilità di usare un proxy diverso per ogni collegamento, importando la lista da un file di testo tipo quello di multiproxy da Internet o inserendo il proxy manualmente prendendolo da servizi disponibili in rete; inoltre abbiamo la possibilità di controllare se il proxy in uso è veramente anonimo o meno.
Tra le sue molte opzioni c'è la possibilità di fare un ping al server, editare i cookie di un sito mentre li accettiamo, attivare una funzione popupkiller, eseguire il comando whois, cancellare ogni traccia della nostra navigazione alla chiusura del browser, e scaricare l'intero sito Web ed i suoi link usando il comando Clone this Web per rileggerlo successivamente con calma. Oppure ancora, è possibile analizzare la struttura del sito in questione. La Search Bar fa qualcosa in più che effettuare una ricerca su Google: nella pagina risultante, infatti, verngono evidenziate tutte le occorrenze della parola cercata.
Inoltre, premendo la combinazione Ctrl + Q il browser scompare dal nostro desktop per ricomparire solo successivamente alla pressione di questa combinazione di tasti (utilissima in ufficio ;-).

Cookie, cronologia, file temporanei: tutte le tracce della sessione di navigazione possono essere eliminate in qualsiasi momento.

Le parole cercate vengono evidenziate all'interno della pagina.

>> Interfaccia funzionale

Per facilitare la raccolta di informazioni o la compilazione di moduli, Touchnet Browser permette di trasportare testi sulla barra indirizzi, sull'edit box, dall'edit box al Web, da sito Web a sito Web, semplicemente trascinandoli da una finestra all'altra. A differenza di Internet Explorer, poi, tutte le pagine vengono aperte all'interno della stessa finestra, e appaiono come una linguetta nella parte superiore. In questo modo si può saltare rapidamente da una pagina all'altra e si possono poi chiudere tutte le pagine contemporaneamente. Si può inoltre scegliere cosa deve caricare ed eseguire dalle diverse pagine Web (foto, video, script java, ActiveX). È inoltre presente la possibilità di richiedere da browser la traduzione di una pagina usando i motori per traduzione di Google o Altavista (auguri!). Utilizzando il motore di rendering di Internet Explorer, ne accetta anche i Preferiti, che vengono sempre presentati in ordine alfabetico così da rendere più agevole il reperimento di quello che interessa. L'interfaccia scelta può essere ampiamente personalizzata, attraverso degli skin che la modificano in modo più o meno drastico. Insomma, chi non si accontenta di Explorer (e fa bene), faccia almeno un giro di prova con questo browser alternativo.

Devilman
devilman1@hackerjournal.it

Reversing, questo sconosciuto

No, il reversing non è un'acrobatica posizione del Kamasutra! E allora cos'è? Vediamolo assieme

Scena finale del primo episodio di Matrix. Neo sta per morire sotto i colpi dell'agente Smith ma solo dopo che il suo cuore smette di pulsare si rende conto veramente della situazione: Matrix non è la realtà, ma solo un software che, in quanto tale, può essere alterato, crackato, riprogrammato. Neo si riprende e da quel momento in poi il suo sguardo è in grado di indugiare dentro Matrix, oltre l'apparenza, oltre la sua interfaccia direttamente dentro il suo codice sorgente. Tale abilità gli consente di dominare il software che lo circonda e diventando pressoché invincibile al suo interno. La finzione cinematografica, in questo caso, rappresenta benissimo la metafora del passaggio dallo stadio di utente (colui che utilizza i programmi) a quello di reverser (colui che smonta, analizza e modifica i programmi a proprio uso e consumo). Chi pratica il reversing, quindi, è un hacker in piena regola, perfettamente in accordo con la definizione del Jargon File e con quella riportata dietro la copertina in ogni numero di questa rivista.

>> Il significato del termine

Ci si riferisce spesso alla programmazione come processo diretto perché, da un'idea originaria, si stila un algoritmo in base al quale si crea il codice sorgente del programma da realizzare che, una volta compilato, produce l'eseguibile vero e proprio. L'ingegneria inversa (traduzione maccheronica di "reverse engineering", sinonimo di "reversing"), invece, si muove esattamente nella direzione opposta: abbiamo a disposizione un programma eseguibile compilato e funzionante e vogliamo ottenerne il listato in linguaggio assembly da cui poter ricavare l'algoritmo originario.

>> Campi di applicazione.

Di reverse engineering non si parla solamente in relazione ai programmi. Si può fare il reversing di un protocollo chiuso di comunicazione, per poter interfacciare il proprio software con altri preesistenti. È accaduto con Samba, con i cloni di ICQ, di eDonkey e di molti programmi famosi.
Nel campo dell'hardware il fenomeno è stato spesso dibattuto nelle aule di tribunale in cui si sono fronteggiati i colossi di Silicon Valley e quelli di Taiwan colpevoli, secondo i primi, di aver sfruttato l'ingegneria inversa per appropriarsi di tecnologie sviluppate dalla concorrenza.
Perfino in guerra, quando viene catturata un aereo nemico, viene studiato a fondo per carpirne i segreti e anche in questo caso si parla di reverse engineering. Sfortunatamente per voi, però, la mia indole è pacifica e da qui in avanti concentrerò l'attenzione sul reversing del software!

>> La situazione in Italia

Il reversing in Italia è sempre rimasto un fenomeno di nicchia, senza mai scomparire né esplodere. Di gruppi hacker ce ne sono molti, ma pochi sono quelli specializzati nel solo reversing. Quei pochi, però, sono veramente di elevatissimo livello, con persone molto capaci e disponibili. Tra i gruppi storici non si può non citare quello dei Ringz3r0, che ha riscosso un notevole successo nel passato e ora si è praticamente smembrato ma i suoi tutorial sono ancora tutti on-line e tutti da leggere! Per un gruppo che non esiste più se ne trova un altro nato da poco, quello dei Protected Mode, altro sito da visitare e pieno di tutorial. Il vero zoccolo duro del reversing italiano degli ultimi tempi, però, ruota attorno a un sito ed un personaggio. Sto parlando di Quequero e dell'Università Italiana del Cracking (UIC) da lui fondata. Qui si possono trovare tutte le informazioni necessarie, molti tutorial e vere e proprie lezioni per tutti i livelli di difficoltà. Ci sono anche vari CrackMe, piccoli programmini che permettono di esercitarsi nel cracking e nel rever-

14_15_hj32_bit 18-08-2003 10:05 Pagina 15

http://www.liberliber.it/biblioteca/tesi/giurisprudenza/diritto_del_lavoro/tutela_giuridica_del_software/html/cap3_7.htm
http://www.tutelautore.it/l63341art63a79.htm

Il reversing e la legge italiana.

La legge 633/41 all'articolo 64 quater traccia il confine entro cui il reversing è legale.

Art. 64-quater
1. L'autorizzazione del titolare dei diritti non è richiesta qualora la riproduzione del codice del programma di elaboratore e la traduzione della sua forma ai sensi dell'art. 64-bis, lettere a) e b), compiute al fine di modificare la forma del codice, siano indispensabili per ottenere le informazioni necessarie per conseguire l'interoperabilità, con altri programmi, di un programma per elaboratore creato autonomamente purché siano soddisfatte le seguenti condizioni:
a) le predette attività siano eseguite dal licenziatario o da altri che abbia il diritto di usare una copia del programma oppure, per loro conto, da chi è autorizzato a tal fine;
b) le informazioni necessarie per conseguire l'interoperabilità non siano già facilmente e rapidamente accessibili ai soggetti indicati alla lettera a);
c) le predette attività siano limitate alle parti del programma originale necessarie per conseguire l'interoperabilità.
2. Le disposizioni di cui al comma 1 non consentono che le informazioni ottenute in virtù della loro applicazione:
a) siano utilizzate a fini diversi dal conseguimento dell'interoperabilità del programma creato autonomamente;
b) siano comunicate a terzi, fatta salva la necessità di consentire l'interoperabilità del programma creato autonomamente;
c) siano utilizzate per lo sviluppo, la produzione o la commercializzazione di un programma per elaboratore sostanzialmente simile nella sua forma espressiva, o per ogni altra attività che violi il diritto di autore.
3. Le cause contrattuali pattuite in violazione dei commi 1 e 2 sono nulle.
4. Conformemente alla convenzione di Berna sulla tutela delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, le disposizioni del presente articolo non possono essere interpretate in modo da consentire che la loro applicazione arrechi indebitamente pregiudizio agli interessi legittimi del titolare dei diritti o sia in conflitto con il normale sfruttamento del programma.

sing in completa legalità senza doverlo fare con programmi commerciali.

>> I programmi del provetto reverser

Il primo è più importante dispositivo che bisogna possedere è… il cervello! Sembra una banale battuta, me è proprio così. Per chi non ha mai programmato, poi, lo sforzo intellettivo potrebbe essere veramente fuori dal comune. Con questo non voglio certo spaventare chi sta leggendo, ma ho notato che i miei amici mi guardano come un marziano quando mi vedono davanti allo schermo a fissare lunghe sequenze di istruzioni in assembly. Una buona conoscenza del linguaggio assembly, infatti, è un prerequisito imprescindibile per chiunque voglia dedicarsi a questo genere di attività.
Dopo la nostra mente, i debugger e i disassemblatori sono i programmi più importanti per potersi dedicare al reverse engineering. Tra i debugger per Windows il più famoso e usato è il SoftICE della Numega, mentre tra i disassemblatori quelli che vanno per la maggiore sono il W32Dasm della URSoft e l'Interactive Disassembler Professional (per gli amici IDAPro) della Datarescue. Sotto Linux la stragrande maggioranza del software è open source, cosa che rende pressoché inutile il reversing. Tuttavia, per quel poco software di cui non sono disponibili i sorgenti, ci sono il GNU debugger, il pICE (un clone del softICE), hexdump ed hexedit (presenti in tutte le distribuzioni) e dasm, un disassemblatore minimale scritto in perl.

>> Come funzionano

Partiamo dal più famoso: SoftICE. È un debugger implementato come kernel driver e, in quanto tale, ha accesso diretto e completo al sistema proprio come un driver. Il grosso vantaggio dei programmi di questo tipo è che permettono di visionare il codice di un programma mentre è in esecuzione, cosa utilissima soprattutto se il programma che si sta analizzando è protetto con determinate tecniche. Alcuni eseguibili, infatti, sono criptati e/o compressi e si scompattano/decriptano solo quando vengono lanciati. Tali programmi, quindi, non possono essere studiati con un tradizionale disassemblatore, ma è necessario un debugger come il SoftICE. Anche con eseguibili non criptati, comunque, SoftICE è uno strumento potentissimo che permette di arrivare rapidamente nella parte del codice che ci interessa. Si può usare, poi, anche per analizzare il funzionamento interno del kernel e dei driver del sistema operativo.
L'Interactive Disassembler è un software completamente diverso dal SoftICE. È un classico ma potentissimo disassemblatore con moltissime opzioni utili. Restituisce dei listati chiari e di ottimo livello. Ha lo svantaggio di essere abbastanza lento, soprattutto se viene usato su eseguibili particolarmente grossi, ma spesso vale la pena di attendere qualche secondo in più, vista la mole di informazioni che può offrire. Un altro vantaggio di IDAPro è la sua versatilità, in quanto può analizzare eseguibili e programmi sia per DOS che per Windows, ma non solo! Supporta moltissime altre architetture hardware, tra cui i PIC della Microchip e gli AVR dell'Atmel. Se quindi volete studiare il contenuto del file flash di qualche smartcard, IDAPro è il software più adatto.
Ultimo, ma non per questo meno importante, è il W32Dasm. Questo nome un po' criptico nasconde uno strumento preziosissimo nelle mani del reverser. Nonostante l'ultima versione risalga al '98 del secolo scorso, riscuote ancora moltissimo successo. È un disassemblatore molto più rapido e molto più semplice da usare di IDAPro e permette anche di caricare un eseguibile e di farlo girare sotto il suo controllo assomigliando, sotto questo aspetto, al SoftICE. Supporta però solo codice a 32bit per Windows e quando funziona da debugger è meno potente di SoftICE, ma la sua velocità, semplicità d'uso e versatilità ne fanno comunque un prezioso alleato del reverser.

>> Conclusioni

Spero che questa carrellata sia stata utile per inquadrare l'argomento e mi auguro di aver suscitato un briciolo di curiosità nel lettore. Se così fosse, penso che potrebbe essere interessante entrare un po' più nell'argomento con degli esempi pratici. Fate sapere a me ed alla redazione cosa ne pensate. Ciao!

fantoibed
fantoibed@spippolatori.com

LINK UTILI
http://quequero.org/UIC

http://www.ph0b0s.itcsalvemini.org/R0Mirror/Ringz3r0

http://pmode.cjb.net/
Protected Mode

MIGMAF:

L'eterna lotta telematica tra spammer e anti-spammer continua. Entrambi affilano le loro armi. Vi raccontiamo l'ultimo episodio della saga.

Se gli spammer creano sistemi sempre più sofisticati per eludere il tracciamento, i loro nemici stanno costituendo comunità sempre più numerose in modo da far fronte sempre più velocemente, con un massiccio scambio d'informazioni, alle nuove insidie dello spammer di turno.

Verso la fine di giugno di quest'anno un gruppo di anti-spammer, facenti capo al gruppo Usenet news.admin.net-abuse.email, nota uno spammer che **sembra essere in grado di spostare il proprio sito da un IP ad un altro con una velocità impressionante** (nel caso specifico un sito hard russo). Nonostante il gruppo avesse denunciato l'accaduto ai provider su cui il sito sembrava trovarsi, questi ultimi non riuscivano a venirne a capo poiché **gli IP denunciati appartenevano a classi di IP utilizzate per le connessioni ad internet dell'utenza privata**.

Richard M. Smith (www.computerbytesman.com) ipotizza allora l'esistenza di **un trojan che faccia da Web server** e su cui venga di volta in volta scaricato in automatico il sito dello spammer. Questa tesi, per quanto possa apparire plausibile di fronte all'eccezionalità del fenomeno descritto, **non convince gli analisti della LURHQ**, un'azienda americana che si occupa di servizi di sicurezza, i quali, messe le mani su una copia del fatidico trojan, recuperato dal computer infettato di un utente di una VPN, analizzano il comportamento dell'eseguibile. Ecco a cosa ha portato questa analisi.

>> Funzionalità di Migmaf

Il risultato più importante dell'analisi del LURHQ è stato la scoperta in base alla quale il **migmaf non è un webserver bensì un webproxy**, perciò, in realtà, quando un utente cerca di connettersi a certi domini, pubblicizzati nelle email di spam, viene indirizzato sui computer infettati di ignari utenti e da questi **reindirizzato sul web server che effettivamente ospita il sito hard**. Ecco il motivo per cui i vari ISP chiamati in causa non riuscivano a trovare il sito incriminato ma si trovavano di fronte alle classi di IP da loro stessi dedicate alle connessioni private.

Il migmaf, inoltre, **rende difficile l'individuazione del server madre** (intendendo per server madre quello in cui si trova il sito hard) anche per l'utente infettato, perché **la connessione tra il migmaf e il server madre avviene in modo "casuale",** cioè vengono scelti 3 valori per ognuno dei 4 ottetti che costituiscono l'indirizzo IP per un totale di 3 x 3 x 3 x 3 = 8 1 combinazioni possibili di cui soltanto una raggiunge l'obiettivo desiderato. Per cui "ascoltare" il traffico di rete per un tempo non adeguato può non portare ai risultati desiderati.

Altro servizio fornito dal migmaf allo spammer è un socks proxy server in ascolto sulla porta 81, che **consente il passaggio di email attraverso il computer infettato** che vengono in questo modo completamente anonimizzate. Il migmaf è inoltre dotato di **un sistema di ottimizzazione delle risorse a disposizione**. Infatti, effettua una verifica della banda disponibile sulla linea ospite inviando una serie garbage data (pacchetti spazzatura) verso la porta 80 del sito Microsoft. Questo è stato intuito dagli uomini della LURHG dalla presenza di questa stringa nel codice del trojan:

```
"disclaimer:
www.microsoft.com used for
bandwith speed testing only"
```

Scopo del messaggio è probabilmente

NEWBIE

IL VIRUS CHE SPAMMA

L'EXPLOIT DI WINDOWS UPDATE

L'exploit di Windows Update è stato scoperto nel giugno di quest'anno e riguarda la possibilità di sfruttare l'aggiornamento di Windows per patchare l'Internet Explorer con un trojan. Questo exploit è stato prontamente utilizzato da alcuni soggetti non ben identificati che hanno inviato ad ignari utenti delle email in cui si invitava ad effettuare un aggiornamento di IE per patchare una vulnerabilità critica. La mail era ben congegnata e rimandava l'utente sul sito windows-update.com, molto simile al vero windowsupdate.com. Ecco un esemplare della mail:

```
Dear Windows User!
New Windows 9x/2000/NT/XP critical patch has been released.
Due to security problems, your system needs to be updated as ear-
lier as possible. You can download an update patch on Windows
Update site: http://www.windows-update.com
Best regards,
Windows Update Group
```

Il sito incriminato è stato prontamente chiuso dal provider ospitante, ma rimane attiva la vulnerabilità che riguarda in pratica tutte le versioni di IE: dalla 5.01 alla 6 comprendendo addirittura la versione 6 di IE installata sull'appena nato Windows Server 2003. La patch (quella vera), corredata di ulteriori informazioni sulla vulnerabilità, la trovate al seguente indirizzo: www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-020.asp

quello di **non attirare l'attenzione di Microsoft** che potrebbe interpretare i garbage data come tentativi di attacchi DoS. Altro elemento da segnalare è che la copia di migmaf su cui si è basata l'analisi del LURHG è stata compilata l'8 luglio 2003. Dal momento che le prime segnalazioni di protesta nel gruppo Usenet citato prima si sono avute nel giugno di quest'anno, è probabile che ancora adesso, mentre stiamo scrivendo quest'articolo, **il migmaf venga modificato e ricompilato per sfuggire al controllo degli antivirus**.
A tutt'oggi non si è certi riguardo alla provenienza del trojan. Qualcuno ha azzardato la Russia, in realtà indotto da uno strano comportamento del migmaf; al momento dell'attivazione su un computer infetto verifica la seguente chiave di registro: **Keyboard Layout****Preload**, se il layout della tastiera risulta quello russo, il programma termina la sua esecuzione.
Questo accorgimento adottato a vantaggio dell'utenza russa non è comunque da considerarsi una prova determinante.

>> Come eliminarlo

Il rapporto del LURHQ termina con alcune indicazioni sulla rimozione di Migmaf: la chiave di registro da eliminare è la seguente:

```
HKEY_LOCAL_MACHINE\Software\M
icrosoft\Current
Version\Run\Login Service =
wingate.exe
```

Il file da eliminare, come avrete potuto intuire dalla chiave di registro, è **wingate.exe** nella cartella system32 di windows. Qualcuno probabilmente ricorderà che il nome di file wingate.exe era già stato utilizzato per nascondere il Lovegate, un worm che possedeva anche le caratteristiche del trojan ponendo in ascolto la **porta 6000** del computer infetto oltre a diffondersi in tutte le cartelle condivise della rete locale. Nonostante ciò, per gli analisti LURHQ **non vi è alcun collegamento fra i due programmi**, almeno da un punto di vista funzionale.
Rimangono però ancora due punti oscuri su cui né il LURHQ né altri soggetti a tutt'oggi sono riusciti a fare chiarezza. Innanzi tutto, migmaf **non dispone di sistemi di autoreplica e autodiffusione** o almeno così è sembrato dal monitoraggio della sua attività, per cui ci si chiede come si sia potuto diffondere. Il LURHQ ha ipotizzato una non precisata diffusione (non precisata soprattutto nei modi) attraverso i **messanger di AOL** oppure **IRC** o **Kazaa**. Un'altra ipotesi, meno legata all'incuria degli utenti delle chat e dei p2p, è **l'utilizzo di un exploit di IE riguardante il Windows-Update** scoperto proprio nel mese di giugno di quest'anno. Nel box troverete maggiori dettagli.
Altro punto oscuro di cui non si parla nel rapporto LURHQ è **il modo con cui viene aggiornato il server DNS che contiene i domini incriminati**. Non si sa infatti se i dati vengono inviati dal migmaf direttamente al DNS oppure se è il server madre ad aggiornarlo. Se avremo notizie in più su questi due punti ve lo faremo sapere in un prossimo articolo.

Roberto 'decOder' Enea
enea@hackerjournal.it

18_19_hj32_tel 18-08-2003 10:06 Pagina 18

Comandare Linux via seriale

Chi l'ha detto che per fare il login remoto sono necessari una rete o un collegamento Internet? Col cavo giusto, e col giusto file di configurazione, si può fare anche attraverso la porta seriale!

Nulla si crea, nulla si distrugge, ma un po' di spazio, volendo, lo si trova sempre! Per quanti computer possano esserci dentro la vostra stanza, **non sarà così difficile trovare dove poter installarvene un altro**; sotto la scrivania o il letto, dentro un armadio o nel cassetto della biancheria, ci sarà comunque posto per un firewall, un router, un server di posta o un web server per i vostri esperimenti... :)
Considerato che in molti casi queste macchine, una volta configurate ed avviate, svolgono il loro compito senza ulteriore intervento da parte dell'utente e che tramite SSH è possibile accedere ad esse da remoto, **solitamente non si prevede nemmeno un monitor ed una tastiera per ciascuno di questi computer**. Fin qui nessun problema, se non fosse che talvolta possono bloccarsi e rendere necessario un intervento diretto; ecco allora che si apre, tra accidenti ed imprecazioni varie, una disperata "caccia al monitor" senza precedenti. Esiste però una soluzione decisamente più efficace, rapida ed indolore; armatevi quindi di buona volontà e **preparatevi a configurare il vostro primo terminale Linux seriale**.

>> Non vedo, non sento, non digito

Linux è un sistema multiutente e multitasking, che permette cioè realmente a più utenti di connettersi alla stessa macchina ed eseguire contemporaneamente più lavori. Per questo vengono messe a disposizione più console virtuali, alle quali è possibile accedere tenendo premuto ALT e contemporaneamente il tasto funzione FX (dove X è il numero della console da utilizzare e il cui numero massimo dipende dalla specifica configurazione del sistema). Tuttavia **le finestre di terminale su display grafico non sono le uniche possibili**; in molti casi infatti vengono utilizzati "stupidi" terminali ASCII connessi proprio tramite porta seriale.
Con l'avvento delle reti, quest'ultima tipologia di terminali è effettivamente caduta in disuso ma in diversi casi è anco-

TUTTO SU GETTY

Sotto Unix non fa molta differenza il fatto che stiate utilizzando un terminale virtuale su un display grafico oppure un terminale vero e proprio. Infatti dopo aver riconosciuto ed inizializzato i diversi dispositivi, il kernel Linux lancia init che a sua volta provvede, tra le altre cose, a generare un processo getty su ciascuna porta terminale attiva. Getty imposta le caratteristiche iniziali della porta (velocità, numero di bit di dati, parità) e stampa un prompt di login. Il nome inserito viene quindi passato al comando login, che richiede quindi la password; dopo averla verificata, questi lancerà quindi la shell predefinita. Infine una volta disconnessi dalla sessione di login su una delle console, il controllo viene restituito a init, che a sua volta rigenera (respawn appunto, come specificato in /etc/inittab) getty e lo mette in ascolto sulla porta del terminale.
Il comando getty, solitamente presente nella directory /sbin, è stato re-implementato più volte e pertanto oggi ne esistono numerose versioni, leggermente differenti tra loro nel comportamento e nella sintassi; insieme all'originario getty troviamo infatti mgetty e il diffuso agetty. Per approfondire ulteriormente l'argomento potete leggere il capitolo 6 dell'ottimo Remote Serial Console How-To del LDP (www.tldp.org/HOWTO/Remote-Serial-Console-HOWTO/) e, ovviamente, la pagina di manuale relativa.

Un vecchio portatile con STLinux all'opera.

ra oggi utilizzatissima se non, addirittura, necessaria. Pensate a una sala contenente rack di server o a un cluster di computer come quelli utilizzati nei centri di calcolo, casi in cui è impossibile prevedere un monitor per ogni computer, o alle soluzioni embedded, che molto spesso non prevedono nemmeno un'uscita video! Senza però allontanarci troppo da casa nostra, potrebbe tornare utile in diversi casi utilizzare ad esempio un vecchio 386 portatile per visualizzare i messaggi di sistema della nostra Linux-box o per avere top sempre in primo piano mentre stiamo cercando di uccidere un maledetto processo zombie avido di risorse.

>> Il cavo

Per prima cosa occorrerà un cavo per connettere le due macchine. Iniziate con il cercare dietro ai vostri computer la porta seriale, altresì conosciuta come COM, ovvero un connettore maschio a 9 o 25 poli (**da non confondere però con la porta parallela**, a 25 poli ma femmina); a questo punto potete recarvi dal vostro negoziante di fiducia e **procurarvi un cavo null-modem** avente le prese femmina e con il giusto numero di pin. Se invece ve la cavate col saldatore, trovate lo schema per costruirne uno all'indirizzo www.mycableshop.com/techarticles/NullModem.htm

>> Il Server...

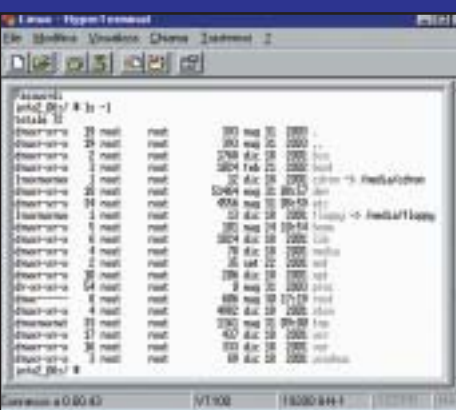
Init è un processo Unix che viene caricato all'avvio del sistema e ha il compito di creare nuovi processi e di lanciare una serie di programmi e script di avvio (o spegnimento). Ogni operazione svolta da init è definita nel **file /etc/inittab**. Nostro scopo è far sì che all' avvio, venga lanciata una nuova console (alla quale corrisponderà un processo **getty**) sulla porta seriale; per far questo modificheremo opportunamente, una volta guadagnati i permessi di root, il file in questione aggiungendo la seguente riga:

```
S1:12345:respawn:/sbin/agetty
-L 19200N8 ttyS0 vt102
```

Non approfondiremo in questa sede la sintassi del file inittab né del comando getty, che può variare in base alla versione installata; osservando comunque le linee simili già presenti in inittab per l'avvio delle console virtuali e leggendo le apposite pagine man (**man getty** o **man agetty** etc..), non dovreste aver problemi. In ogni caso dovrete specificare come parametri la velocità del terminale (nel nostro caso **19200bps**, **No** bit di parità, **8 bit** di dati), la porta seriale (**ttyS0** corrisponde ad esempio alla **COM1**, **ttyS1** alla **COM2** e così via) e il tipo di terminale (il diffuso **DEC VT100** in questo esempio); annotatevi le impostazioni del server, poichè serviranno per configurare anche il terminale nello stesso modo! A questo punto potete salvare il file, uscire e riavviare il PC o, più semplicemente, segnalare ad init l'avvenuta modifica della configurazione digitando:

```
# kill -HUP 1
```

Questo vi consentirà di fare il login da terminale una volta che il vostro computer sarà avviato, ma non potrete ancora vedere i messaggi di boot del kernel (anche se potete sempre usare **dmsg**...). Provate quindi ora a riavviare e utilizzate il boot loader per passare al kernel i seguenti parametri:

```
console=tty0
console=ttyS0,19200n8
```

Il nostro pinguino ha conquistato anche Windows!

Perchè utilizzare due monitor quando ne basta mezzo?

In questo modo tutti i messaggi di avvio verranno mostrati sia sulla prima console virtuale sul vostro monitor, sia sul terminale seriale. Se quest'opzione dovesse rivelarsi necessaria, potete aggiungere i parametri al file di configurazione del vostro boot loader per abilitarla di default.

>> ...e il terminale

Per quanto riguarda il terminale, le possibilità sono molteplici. Gli utenti Windows potranno utilizzare **HyperTerminal** o **TeraTerm** (**http://hp.vector.co.jp/authors/VA002416/teraterm.html**), mentre i linuxiani avranno sicuramente installato **minicom** sulla propria macchina. In alternativa esiste **Kermit** (**www.columbia.edu/kermit**), disponibile praticamente per ogni sistema operativo. Infine vi è **STLinux**, una mini-distribuzione funzionante da floppy creata da J. Bartelett che permette di trasformare ogni PC in un terminale in pochi secondi e senza alcun intervento da parte dell'utente. Vi consigliamo caldamente di provarla scaricando dall'home del progetto (**http://members.wri.com/johnnyb/seriallinux/**) l'ultima versione.

Come già detto, **ricordatevi di impostare il terminale in modo che i parametri di configurazione corrispondano a quelli del server**.

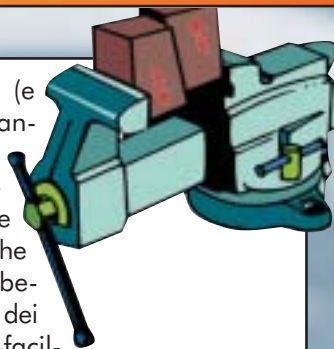
A questo punto siete pronti ad eliminare qualche monitor di troppo liberando così un po' di spazio... magari senza riempirlo subito con un altro computer! ;)

Lele

20_21_hj32_pass 18-08-2003 10:07 Pagina 20

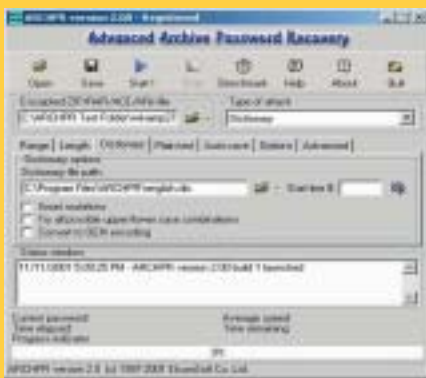
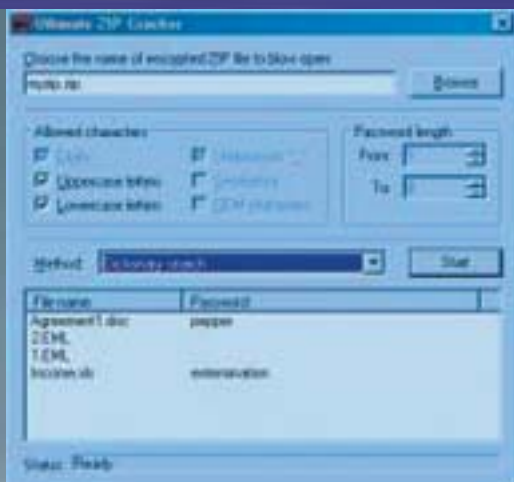
GRIMALDELLI DIGITALI

Possono spremere tutte le risorse del processore, e impiegarci giornate intere, ma raggiungono quasi sempre il loro scopo: violare la password di un archivio compresso.

A chi non è mai capitato di dimenticare la password che si era impostata per un file ZIP o ARJ? E quale rabbia più forte di quella di non poter recuperare i propri preziosi dati?
Fortunatamente per gli utenti e gli amministratori di sistema un po' sbadati che hanno perso le password dei propri archivi (e purtroppo anche per i lamer che vogliono aprire gli archivi che non dovrebbero), esistono dei programmi facilmente reperibili sul Web che possono scoprire le preziose parole segrete senza troppi problemi.

>> Come funzionano

Questi software, generalmente detti Password Cracker, sono stati scritti appositamente per trovare le password dei file protetti: sul Web vengono pub-

ADVANCED ARCHIVE PASSWORD RECOVERY

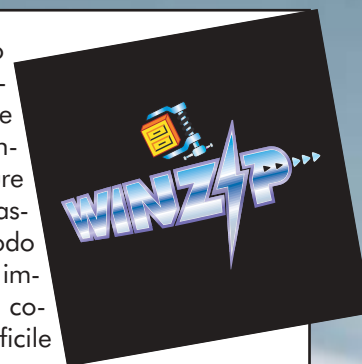
www.elcomsoft.com/prs.html
Prezzo: 60 $

Probabilmente il miglior software attualmente in circolazione per scovare le password degli archivi compressi. Dal Web è possibile scaricarne una versione dimostrativa di 30 giorni, dopodiché si dovrebbe acquistare il prodotto completo per continuare ad usarlo. Advanced Archive Password Recovery permette ri ritrovare le password degli archivi ZIP, ARJ, RAR e ACE con diversi metodi di attacco a seconda delle esigenze dell'utente. Il sistema di ritrovamento della password può essere basato sull'uso di un dizionario, un file di testo contenente un elenco di parole frequentemente usate come password (possono anche essere centinaia di migliaia), e se l'utente che ha settato la password ha utilizzato una particolare parola, questa verrà scovata in pochi minuti. In alcuni casi molto più lento ma matematicamente infallibile è il secondo tipo di attacco usato da Advanced Archive Password Recovery: il Brute-Force, che prova tutte le possibili combinazioni di caratteri fino ad arrivare a quella che corrisponde alla password da inserire! Punti di forza di questo programma sono la facile e veloce interfaccia grafica, la sua estrema velocità (su un computer ad 1 GhZ, riesce a provare circa 15 milioni di password al secondo), la possibilità di scovare anche le password degli archivi Self-Extracting e le opzioni che l'utente può settare per rendere più veloce il ritrovamento della password, come la lunghezza della parola segreta e i caratteri da usare per scovarla. Infine si può interrompere l'attività del programma in qualunque momento e riprenderla quando si vuole senza dover ricominciare da capo la ricerca della password. La versione dimostrativa di Advanced Archive Password Recovery può essere scaricata dal sito del produttore.

blicamente sventolati per lo scopo legittimo di ritrovare le paroline segrete di utenti sbadati che le hanno dimenticate o perse, ma sono spesso segretamente utilizzati da piccoli lamer che si intrufolano negli archivi altrui. Nei box sono descritti alcuni software in grado di scovare in meno di un'ora la password di un archivio contenente cinque o più file. Come accennato all'inizio, questi programmi possono rivelarsi delle armi a doppio taglio: se da un lato sono strumenti indispensabili per non perdere i dati di cui si è smarrita la password, dall'altro possono essere utilizzati illegalmente per violare la privacy degli utenti accedendo ai loro archivi protetti. I Password Cracker sono in grado di effettuare diversi tipi di attacco a seconda delle informazioni che si dispongono sulla password. Per rendere più veloce la ricerca, si può impostare la lunghezza della password o il tipo di carattere con cui è scritta, se si tratta di una data, di una parola o di una sequenza di numeri. Nel caso in cui non si abbia alcuna informazione a riguardo, è possibile effettuare un attacco BruteForce che, pur impiegando molto tempo a terminare l'operazione, assicura all'utente un risultato positivo, dato che è in grado di testare tutte le combinazioni possibili di caratteri alfanumerici e non. Con processori potenti il lavoro si velocizza, ma se si dispone di un vecchio computer l'operazione potrebbe durare anche diversi giorni. In media, i Password Cracker sono in grado di testare migliaia di combinazioni al secondo ma, specialmente se la password è molto lunga, le combinazioni possono raggiungere anche i 20 milioni di miliardi.

>> Niente password banali

Poichè accade di frequente che un software per scovare le password degli archivi non venga usato per scopi legali, ma per scoprire la password di qualcun altro, è bene pensare di invertire i ruoli e trovarsi nei panni della vittima.

A questo punto bisogna pensare a come rendere più sicure le proprie password, in modo da rendere impossibile o comunque difficile che qualche malintenzionato riesca ad avere accesso ai nostri dati.
Ecco perciò alcuni consigli:

- non usare come password parole che vi riguardano e che potrebbero essere facilmente scoperte da chi vi conosce: nome, data di nascita, indirizzo, numero di telefono e così via;
- non usare termini comuni sia in italiano che in altre lingue facilmente individuabili anche dal più banale password cracker;
- essere sicuri di impostare sempre le password con una lunghezza non inferiore a 7 caratteri;
- usare nelle password diversi tipi di caratteri, creare combinazioni di lettere maiuscole e minuscole con l'aggiunta di numeri, simboli non alfanumerici (come @ o #) e caratteri Ascii.

{RoSwEIL}

ULTIMATE ZIP CRACKER

www.vdgsoftware.com
Prezzo: 29 $

Altro programma che si fa spazio tra i software del suo genere per l'enorme efficacia è Ultimate Zip Cracker. Se da una parte la presenza di un programma di questo tipo può far cadere il mito della sicurezza dei nostri preziosi file, dall'altra può essere davvero la salvezza quando "non riusciamo a ricordare quale password abbiamo usato, o quando un collega ci ha lasciato da mesi e non ha avuto il buon senso di sbloccare i suoi archivi", commentano i produttori. Oltre agli archivi ZIP e ARJ, questo software è in grado di lavorare anche sui file di Word ed è caratterizzato dalla particolarità di garantire maggiore probabilità di successo se gli si forniscono più file bloccati con la stessa password. Anche con Ultimate Zip Cracker è possibile scegliere quale metodo di attacco utilizzare: BruteForce, avvantaggiato dalla velocità, che gli permette di provare anche due milioni di combinazioni al secondo; Smart Search, con cui prova un elenco di parole utilizzate di frequente per proteggere i propri file; Simple Dictionary, con cui prova circa 140.000 parole contenute in un file di testo. Caratteristiche particolari di questo software a pagamento sono due originali tipi di attacco: Date Search consiste nel testare oltre 5.000 diversi formati di data (nel caso in cui si sa che la password è una data), Customized Search permette di personalizzare la ricerca per rendere più facile il ritrovamento della password. Senza dubbio i punti di forza del programma sono tanti e convincenti, ma ha un punto debole piuttosto consistente: la versione di prova che si può scaricare non permette di trovare la password di un file, o meglio, Ultimate Zip Cracker trova la password ma non la mostra a ricerca ultimata se il software non viene registrato e acquistato per 29 dollari. Mostra invece una serie di documenti che testimoniando la sua efficacia e il suo buon funzionamento.

22_hj32_porta 18-08-2003 10:08 Pagina 22

NEWBIE

Alla ricerca della porta aperta

Tutti almeno una volta avrete sentito parlare di port scanning e nmap. In questo articolo analizziamo le principali tecniche di scanning adoperate da nmap.

Come tutti saprete già, il port scanning ci **permette di sapere quali porte sono aperte**, e di conseguenza quali servizi sono attivi. Nmap usa diversi metodi di scansione, tra cui per esempio il **SYN scan**, **TCP connect()**, **FIN scan**, eccetera. Ognuno di questi metodi necessita di poteri di root, tranne il TCP connect().

>> TCP connect()

Questa è la tecnica di scansione più semplice, attuabile con un qualsiasi programma che tenti una connessione verso un host. Se la connessione va a buon fine, vuol dire che la porta è aperta. Essa si basa sul "three way handshake". Il suo funzionamento è illustrato nelle immagini.
Questa tecnica di scanning è quella più facilmente individuabile; qualsiasi amministratore non cieco, e ogni rilevatore di intrusioni che si definisca tale, si insospettirebbe a vedere lo stesso host che si connette a parecchie porte.

```
# nmap -sT host
```

>> SYN scan (o half-open scan)

Questo tipo di scan attua una "mezza connessione". Viene inviato un pacchetto con la flag SYN attiva: se il server risponde con le flag SYN e ACK attive vuol dire che la porta è aperta; l'attaccante provvederà quindi a inviare un pacchetto con la flag RST, così non porterà a termine la connessione. Se il server risponde con le flag ACK e RST, la porta è chiusa. Rispetto alla precedente, per l'attaccante questa tecnica ha il vantaggio che non tutti i server registrano i tentativi di connessione non andati a buon fine.

```
# nmap -sS host
```

>> UDP scan

Grazie a questa tecnica un attaccante è in grado di sapere quali porte UDP sono aperte. Il suo funzionamento è abbastanza semplice. Invia un pacchetto UDP di 0 byte; se la porta è aperta, non avrà nessuna risposta, altrimenti riceverà un pacchetto ICMP port unreachable. Questo tipo di scansione è molto lento, poiché molti sistemi utilizzano un suggerimento contenuto nella RFC 1812, che limita l'ammontare dei messaggi d'errore ICMP. Su sistemi Windows, come al solito, questo problema non si presenta, visto che Microsoft non ha seguito il suggerimento, consentendo all'attaccante una scansione molto più veloce.

```
# nmap -sU host
```

>> Window scan

Serve a determinare se una porta è filtrata o meno, e anche se è aperta. Questo tipo di scansione si basa su un'anomalia della dimensione della finestra TCP. Tra i sistemi vulnerabili a questa falla troviamo molti derivati di BSD, ma non solo: FreeBSD, NetBSD, OpenBSD, OS/2, MacOS, SunOS 4.x, Amiga, BeOS.

```
# nmap -sW host
```

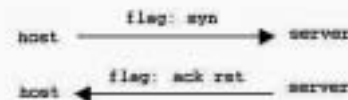
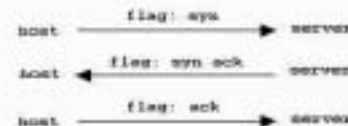
Adesso analizzeremo i metodi di scan più insidiosi, ovvero il FIN scan, lo Xmas Tree e il Null scan. Dico più insidiosi perché è più difficile che questi pacchetti vengano loggati. Come la precedente Window scan, queste tecniche non funzionano su sistemi Microsoft.

>> FIN scan

Inviamo un pacchetto con la flag FIN attiva, se la porta è aperta non riceveremo nulla, se invece fosse chiusa riceveremmo un pacchetto con la flag RST attiva.

```
# nmap -sF host
```

host — flag: syn → server
host ← flag: syn ack — server
host — flag: ack → server

host — flag: syn → server
host ← flag: ack rst — server

>> Xmas Tree

Le flag attive stavolta sono tre: FIN, URG, PUSH. Se non riceviamo nulla la porta è aperta, se invece riceviamo un RST la porta è chiusa.

```
# nmap -sX host
```

>> Null scan

Il funzionamento è identico ai due precedenti (nulla = aperta, RST = chiusa). Il pacchetto da inviare non avrà nessuna flag attiva.

```
# nmap -sN host
```

norloz

23_25_hj32_sql 18-08-2003 10:09 Pagina 23

Sql e web: un'accoppiata rischiosa

I database che stanno dietro ai siti Web dinamici sono spesso vulnerabili ad attacchi SQL Injection, che consistono nell'iniettare codice nel campo di un form.

Con lo sviluppo e la diffusione del Web è cresciuta sempre di più l' esigenza di avere siti Web dinamici, cioè con pagine che permettano di interagire con l'utente e possano offrire determinati servizi. In seguito a questa necessità sono nate nuove tecnologie e nuovi linguaggi che consentono di soddisfare queste richieste.
Questi linguaggi offrono numerose possibilità, e permettono tra le altre cose di **interfacciarsi ai database attraverso SQL,** in modo da poter creare motori di ricerca, database di utenti, eccetera.
Tutte cose molto interessanti, ma come l'esperienza insegna, se queste innovazioni non sono ben gestite possono essere delle gravi falle di sicurezza.

>> SQL Injection

Uno dei problemi più comuni dovuto a un mancato controllo sulle stringhe SQL in una pagina Web, prende il nome di **SQL Injection**. Le tecniche di exploit basate su SQL injection consistono nel far eseguire al server Web oppurtune query SQL che permettano di effettuare determinate operazioni senza averne i permessi, come ad esempio avere accesso ad un area ristretta di un sito Web senza conoscere la password, oppure visualizzare i dati presenti in un database, o ancora inserire opportuni record senza averne l'autorizzazione.

>> Capire il problema

Inziamo subito a capire come questo può accadere con un esempio: supponiamo di realizzare una pagina Web di login. Una delle tecniche per verificare se un utente è presente o meno nel database consiste nel selezionare con una query tutte le righe che hanno il campo login e password uguale a quelli inseriti dall'utente; se come risultato della query si ottiene la riga della tabella che contiene le informazioni relative a quel determinato utente, allora il login è consentito; se invece non si ottiene nulla, allora il login è negato.
Per fare questo bisognerà fare una query di questo tipo:

```
Select * From NomeTabella Where Login =
'VarLogin' AND Password = 'VarPassword'
```

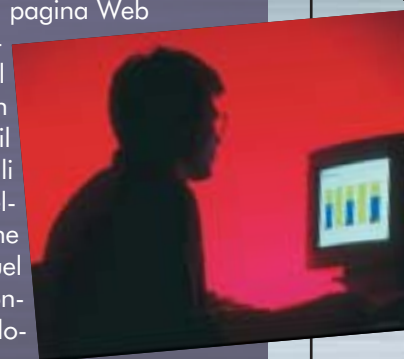
Ovviamente **VarLogin** e **VarPassword** saranno le due variabili che vengono passate dal form della pagina Web.
Ora immaginiamo che, quando si deve autenticare, l'utente inserisca sia nel campo "Login" che nel campo "Password" una stringa del tipo:

```
ciao' OR 'a'='a
```

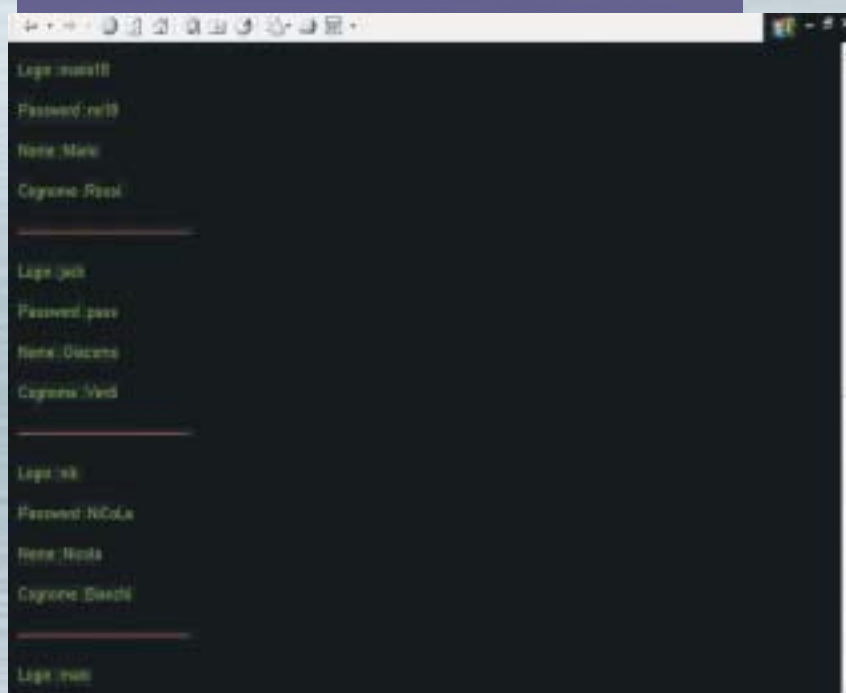
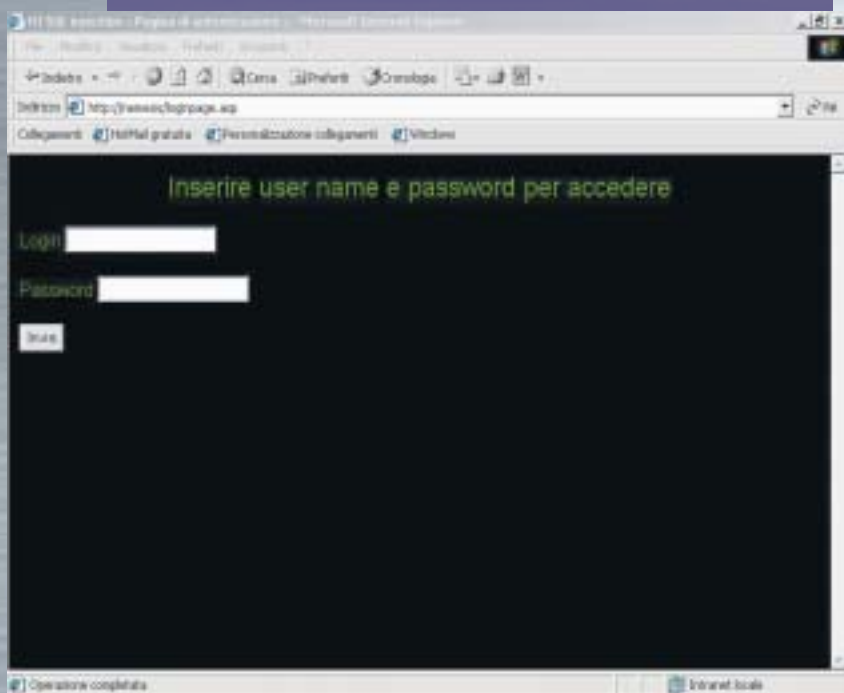
La query che ne risulta è la seguente:

```
Select * From NomeTabella Where Login =
'ciao' OR 'a'='a' AND Password = 'ciao' OR
'a'='a'
```

(Codice A)

23_25_hj32_sql 18-08-2003 10:10 Pagina 24

L'operatore logico OR risulta verificato se almeno una o entrambe le condizioni sono verificate, e dato che la condizione **'a'='a'** è sempre vera, significa che il risultato della query non sarà vuoto e quindi **l'accesso è consentito**.
Come potete subito intuire, le tecniche di SQL injection possono essere raggruppate in due grandi insiemi: quelle tese a visualizzare informazioni che normalmente non dovremmo vedere, e quelle tese a ottenere l'accesso o i privilegi in zone in cui non siamo autorizzati.

Se il sito Web è affetto da questo problema, otterrete qualcosa del tipo:

```
Tipo di errore:Microsoft OLE DB Provider
for ODBC Drivers
(0x80040E14)[Microsoft][Driver ODBC
Microsoft Access] Errore di sintassi (ope-
ratore mancante) nell'espressione della
query 'Login= 'pippo'blablabla ' AND
Password = '''.
```

>> SELECT injection

Supponiamo di avere di fronte a noi la schermata di login di Figura 1 (che potrete trovare per i vostri esperimenti su www.wowzone.too.it, raggiungibile anche dalla sezione Contenuti Extra del sito di Hacker Journal). Inserendo il nostro login e la nostra password, possiamo avere accesso ai dati (per esempio per poterli modificare).
Per prima cosa bisogna capire se la pagina ha questo tipo di problema; il modo più rapido e banale per capirlo è inserire nel campo "login" o nel campo password **una stringa che risulterebbe errata a SQL** e vedere se ci restituisce un errore del gestore DBMS. Quindi inseriamo subito nel campo login o nel campo password una stringa del tipo **"pippo'blablabla"**. Questa stringa ovviamente realizzerà una query errata, poiché nel Where della query cercherà di verificare qualcosa del tipo:

```
Where Login = 'pippo'blablabla
```

(Codice B)

Ora che abbiamo la verifica che la pagina molto probabilmente è vulnerabile da SQL injection, proviamo a realizzare un accesso inserendo una stringa come quella già presentata, in modo da ottenete una query come quella precedente (Codice A). Come vedete dalla figura 2, ecco che abbiamo di fronte le informazioni su tutti gli utenti presenti nel database.
Come noterete, lo stesso codice può essere usato anche per ottenere un accesso non autorizzato.
Analizziamo meglio la stringa che mettiamo per ottenere una query tipo quella del Codice A; nell'esempio passiamo la strin-

ATTACCHI AVANZATI

Se il DBMS usato è MS SQL server è possibile eseguire alcuni attacchi avanzati. Utilizzando il comando EXEC è possibile attivare delle stored procedures. SQL server ha alcune procedure di default che permettono di fare diverse cose molto pericolose. Per esempio, la procedura xp_cmdshell permette di eseguire comandi della shell DOS (per esempio, EXEC master..xp_cmdshell dir c:\ elenca i file sul disco fisso).
Vi sono anche alcune procedure per il controllo del registro, ad esempio xp_regread, xp_regwrite ecc.

ga **ciao' OR 'a'='a** .Notate come sia molto importante il modo in cui sono gestiti gli apici (') nella query. Qui presupponiamo che il programmatore abbia preparato una stringa da passare al DBMS di questo tipo:

```
"SELECT * FROM tabella WHERE Login = ' " +
variabiledilogin "' AND Password = '" +
variabiledipassword "'"
```

dove **variabiledilogin** e **variabiledipassword** sono le stringhe di login e di password che noi passiamo nel form. Come si può vedere qui, gli apici (') di apertura e di chiusura delle stringhe da confrontare sono già inclusi nella stringa: ecco perché nella nostra stringa evitiamo di aprirlo all'inizio e chiuderlo alla fine. Nonostante questo sia il modo più diffuso per passare una stringa al DBMS, diversi programmatori utilizzano alcune accortezze per scoraggiare i meno esperti, per esempio passando i parametri aprendo e chiudendo una parentesi:

```
"SELECT * FROM tabella WHERE Login = (' "
+ variabiledilogin "') AND Password = ('" +
variabiledipassword "')"
```

In questo modo la stringa di prima restituirebbe un errore dal DBMS, ma ciò non significa che il sito non sia vulnerabile da SQL injection.

>> INSERT injection

Quanto detto per la select è valido anche per altri tipi di query, per esempio in un form di registrazione che aggiungerà dei dati ad una tabella ci sarà una query del tipo:

```
INSERT INTO
prova(Login,Password,Nome,Cognome)
Values('Varabilelogin','VariabilePassword',
'VariabileNome','VariabileCognome')
```

E ci saranno le relative textbox nelle quali inserire i quattro parametri. Se il DBMS utilizzato dal sito supporta le query nidificate, si può passare in tutti i campi del form o solo in quelli che ci interessano una stringa del tipo:

```
+SELECT campocheciinteressa FROM prova
LIMIT 1+'
```

Questa stringa preleverà la prima riga del campo interessato e la passerà come parametro nel form (bisogna conoscere però il nome del campo e il nome della tabella). Nel caso precedente si possono passare, per esempio, nome e cognome del primo utente estratto: la cosa può sembrare abbastanza irrelevante a prima vista, perché se non vogliamo registrarci con il nostro nome è sufficente che ne scriviamo uno falso senza ricorrere a SQL injection; ma immaginiamo di registrarci su un sito per fare acquisti in rete e di poter prelevare il codice della carta di credito da passare come parametro, questo potrebbe essere un problema più grave.

>> Altri tipi di attacchi SQL injection

Visto che, come abbiamo notato, si può estendere tutto questo a un qualsiasi costrutto SQL, è possibile modificare dati o cancellarli in modo abusivo sfruttando query di **UPDATE** e **DELETE** eccetera. Oppure si possono passare query completamente diverse chiudendo la query in esecuzione al momento e aprendone un'altra (tutto questo è possibile solo se queste funzioni sono supportate dal DBMS).
Se per esempio vi è una generica select del tipo:

```
SELECT * FROM tabella WHERE campo1 = '
+Variabile+ '
```

Si può passare a "Variabile":

```
';INSERT INTO tabella(campo1,campo2)
VALUES('boh','nonso')—
```

con '; chiudiamo la prima query, dopo di che si fa la seconda query. Le due - - alla fine dicono al DMBS di ignorare tutto quello che c'è dopo.

>> Conclusioni

Con queste poche righe spero di avervi fatto capire quanto sia importante effettuare controlli sulle stringhe che vengono passate al DBMS. Ogni campo del form dovrebbe quindi essere verificato, e riportare un errore se contiene caratteri vietati (gli apici per esempio), o parole che in realtà sono istruzioni SQL. Particolare cura dovrà essere posta nei campi del modulo di autenticazione.
Vi lascio infine con una serie di link per approfondire l'argomento e, se volete provare alcune delle tecniche qui esposte, ho realizzato una pagina Web apposta che potrete trovare all'indirizzo **www.wowzone.too.it**.

Roberto (WhisperOfWind) Valloggia
whisperofwind@libero.it

LINK UTILI

Per chi non conosce il linguaggio SQL o per chi vuole ripassarlo:
www.manuali.net
www.html.it
http://guide.supereva.it/database/sql/

Chi vuole approfondire l'argomento SQL Injection:
http://guide.supereva.it/database/sicurezza/
www.spine-group.org/proggy/sql_injection.pdf
http://www.itvirtualcommunity.net/educational/sql_injection.htm

Variabili & tipi di dati

Nessun programma può funzionare senza conoscere i dati che dovrà elaborare: per questo, si utilizzano variabili e costanti. Facciamo la loro conoscenza.

Nel numero scorso abbiamo visto come analizzare un problema e scomporlo in una serie (sequenza) di istruzioni. Siamo quindi in grado di **realizzare un diagramma di flusso che, graficamente e sinteticamente, illustra la risoluzione del problema**.
Ora dobbiamo tradurlo sotto forma di programma e di codice attraverso un qualsiasi linguaggio da noi scelto.
Per capire molti dei concetti che andiamo (e andremo) a introdurre, teniamo presente che l'utilizzo primordiale dei computer era quello di **valido aiuto per risolvere problemi matematici**; basti pensare che nella lingua italiana, la fedele traduzione del termine inglese computer è "calcolatore". Di conseguenza, parte della terminologia informatica trae origine dal lessico matematico.

>> Dati e variabili

Per risolvere un qualsiasi problema, dovremo elaborare una serie di dati che saranno forniti dall'utente e che vanno sotto il nome di **input** (dati di ingresso, di immissione), per essere poi elaborati e fornire un **output** (risultato di uscita).
I dati forniti dall'utente dovranno essere memorizzati e ad essi dovrà essere associato un nome formale, che possa permettere di identificare il dato all'interno del programma stesso. Un po' come si fa appunto in matematica, quando per rappresentare dei numeri si usano delle costanti (P greco, e…) o variabili (x, y, z…).
Stiamo in questo modo definendo la tipologia dei dati che saranno trattati dalla variabile e nominando le variabili che caratterizzano il nostro problema.
La **scelta del nome della variabile è naturalmente delegata al programmatore** che però dovrà attenersi a delle regole (generalmente valide per tutti i linguaggi):

1) Il primo carattere che identifica una variabile non deve essere un numero (tipicamente deve essere una lettera, ma a volte è accettato anche il carattere _ underscore).
2) Il nome può contenere lettere, numeri e caratteri speciali (non tutti i caratteri speciali sono accettati universalmente

LE UNITÀ DI MISURA INFORMATICHE

L'unità fondamentale (l' "elettrone informatico") è il bit che può essere 0 o 1.
Il bit è l'unita preferita dai gestori ADSL, con il quale pubblicizzano le prestazioni della connessione (il numero più è grande, più fa effetto!).
8 bit costituiscono 1 byte.
1024 byte costituiscono 1 kilobyte (KB), anche se nel linguaggio comune tale valore si approssima con 1000; ma è solo una approssimazione, non è la verità, quindi attenzione!
1024 KB costituiscono 1 megabyte (MB)
1024 MB costituiscono 1 gigabyte (GB)
E poi si potrebbe continuare con i classici nomi (presi in prestito dalla fisica): tera, peta, esabyte e via dicendo.

PI = 3.14159

Lettura Scrittura

Una costante non può variare il suo valore nel corso del programma.

Variabile

Lettura Scrittura

Per tutte le variabili all'interno del programma è possibile modificare il contenuto.

DICHIARAZIONE DELLE VARIABILI

Non tutti i linguaggi necessitano una dichiarazione delle variabili; per esempio, nel python e nel perl non si ha una fase dichiarativa. Nel linguaggio C e nel pascal la dichiarazione è obbligatoria.
Come al solito il Visual-Basic è sempre una via di mezzo (fra il vecchio Basic e gli altri linguaggi) e quindi la dichiarazione può essere resa obbligatoria (tramite il comando option explicit), oppure no.
Ma, come abbiamo visto, il non rendere obbligatoria la dichiarazione è solo uno svantaggio. Attraverso una dichiarazione, il compilatore ci segnala se una variabile è stata dichiarata ma non utilizzata (generalmente come "warning" ossia come avvertimento) e se una variabile è utilizzata ma non dichiarata (come errore).
Il tenere sotto controllo la dichiarazione delle variabili permette anche di eliminare noiosi errori del tipo:

Dichiaro le variabili prezzo1, prezzo2, totale (somma dei prezzi)
prezzo1 = 5
prezzo2 = 2
totae = prezzo1 + prezzo2 (attenzione all'errore ortografico nel nome della variabile totale!)
Stampa totale (viene visualizzato 0, quando ci aspetteremmo 7)

Ma se la dichiarazione fosse stata obbligatoria, il compilatore ci avrebbe segnalato l'errore (variabile "totae" non dichiarata) e il warning (variabile "totale" dichiarata ma non utilizzata). Anche se questo è ovviamente un problema risolvibile nel giro di mezzo secondo, le cose non risultano così ovvie e di facile soluzione nel caso in cui la complessità del programma sia di gran lunga superiore.

dai vari linguaggi; quindi in generale attenersi al solo utilizzo del carattere _ ed evitare assolutamente gli spazi).
3) Contenere la lunghezza del nome della variabile (generalmente non superiore a 255 caratteri).

Il nome della variabile deve essere **significativo** (deve cioè ricordare il dato che andrà a contenere) e **non eccessivamente lungo**, perché potrebbe aumentare notevolmente la probabilità di errori ortografici. Nel linguaggio C, per esempio, vengono considerate identiche due variabili che hanno i primi 31 caratteri del nome uguali. Inoltre, il C distingue tra lettere minuscole e maiuscole (case sensitive), per cui "**SOMMA**" e "**somma**" sono due variabili differenti.

>> Qualcosa da dichiarare?

Solitamente, le variabili usate in un programma devono essere definite a priori. Questa fase, detta appunto "**dichiarazione delle variabili**" è **obbligatoria e necessaria in quasi tutti i linguaggi** (vedere box per chi fa eccezione), ed è posta all'inizio del programma.
Nel corso del nostro programma, potremmo aver bisogno di utilizzare dati che possano variare il loro valore, e quindi sono delle variabili vere e proprie, e di richiamare un dato che risulti fisso nell'intera soluzione del problema (e non modificabile ad esempio attraverso una ri-assegnazione) e quindi definito in fase dichiarativa come una costante. Per fissare l'idea di che cosa possa essere una costante, pensate ad un'analogia matematica, ad esempio al P greco (3.14159….) oppure all'accelerazione di gravità (g, 9,81 m/s2).
Tipicamente, in un qualsiasi linguaggio, la fase dichiarativa di una costante è schematizzabile nella seguente maniera:

```
parola_chiave_linguaggio
nome_della_costante =
valore_assegnato (o simili)
```

Esempio nel linguaggio C

```
#define PI 3.14159
```

Esempio in Pascal

```
const PI = 3.14159;
```

Esempio in Visual Basic

```
Const PI = 3.14159
```

Mentre la dichiarazione di una variabile è del tipo:

```
parola_chiave_linguaggio
nome_variabile tipo_variabile
(o simili)
```

Esempio nel linguaggio C

```
int giorno, mese, anno;
```

Esempio nel Pascal

```
var numero, somma: integer;
```

26_28_hj32_prog 18-08-2003 10:12 Pagina 28

TIPI DI DATI

Solitamente, nella fase di dichiarazione di una variabile bisogna indicare anche quale tipo di dati essa andrà a contenere (numeri interi, decimali, stringhe di testo o altro). Ogni linguaggio ha delle piccole differenze (vedi sotto), ma a grandi linee questi sono i tipi di dati più diffusi.

NUMERICHE

Byte da 0 a 255 (1 byte)
Interi (integer, int) da – 32.768 a 32.767 (2 byte)
Long da – 2.147.483.648 a 2.147.483.647 (4 byte)
Float, single da –3,402823E+38 a –1,4011298E–45 per valori negativi; da 1,4011298E–45 a 3,402823E+38 valori positivi (4 byte)
Double (8 byte)

ALFANUMERICHE

Char qualsiasi carattere alfa-numerico (1 byte)
String (lunghezza della stringa, tipicamente al massimo 65.400 caratteri)

LOGICHE

Boolean (2 byte) variabile logica (vero, falso)

Come dicevamo, la schematizzazione riportata sopra è puramente indicativa in quanto la tipologia di variabili può variare da linguaggio a linguaggio.
Ad esempio in Pascal vi è la tipologia real (6 byte) e non si fa distinzione fra long, single e double.
Il byte e lo string non sono ad esempio presenti nel linguaggio C. Per quanto riguarda il C le stringhe sono definite in altro modo (vedremo nel prossimo articolo come).

Esempio in Visual Basic

```
Dim nome_persona As String, Mese As Integer
```

In apparenza, la fase dichiarativa **potrebbe essere noiosa**, ma in realtà **ha una serie di vantaggi non indifferenti**:

1) Permette al programmatore e in generale a chi ha accesso al codice sorgente di **conoscere la natura di una variabile** (numerica o alfanumerica).
2) Se per le variabili si sceglie un nome significativo e lo scopo della variabile è opportunamente commentato, **si aumenta notevolmente la leggibilità del programma** e quindi se ne semplifica la correzione e manutenzione (eventuali versioni successive).
3) Permette di determinare se una variabile all'interno del programma **è trattata in maniera coerente con quella che è la sua natura dichiarata**. Se ad esempio abbiamo definito una variabile come numero intero, non potremo assegnare ad essa un valore numerico non intero (es: 5,678), né tantomeno assegnare un valore alfanumerico senza evitare che il programma vada in errore.
4) Inoltre, a seconda della tipologia della variabile, **sono consentite o meno delle operazioni**. Ad esempio due numeri possono essere addizionati o moltiplicati, ma due stringhe (dati alfanumerici) possono essere sommate (dove l'operazione prende il nome di concatenazione), non ha senso moltiplicarle.
5) Informa il computer di riservare uno spazio di memoria per quella determinata variabile (non tutte le variabili occupano lo stesso spazio in memoria: vedi riquadro in queste pagine).

Esempio di codifica in formato binario ad 8 bit (1 byte) di un carattere alfabetico.

>> Problemi di memoria

Quest'ultima affermazione implica un'altra operazione che è generalmente buona norma eseguire, ossia quella della inizializzazione delle variabili. Infatti nel momento in cui il computer viene a conoscenza della presenza di una variabile, le assegna una porzione di memoria. Il problema è che **la memoria potrebbe essere sporcata da risultati di operazioni condotte in precedenza**, magari da altri programmi. Conseguenza di ciò è che la variabile che noi abbiamo dichiarato nasce con un valore che sicuramente sarà diverso da quello che dovrebbe essere il suo reale contenuto.
Invece, nel momento in cui inizializziamo la variabile, le andiamo ad assegnare un valore e puliamo la memoria riservata alla variabile da eventuali residui che in inglese prendono il nome di "garbage" (spazzatura). Va sottolineata la particolarità del linguaggio C, che supporta le assegnazioni multiple (esempio a = b = c =10).
Nel prossimo articolo prenderemo in esame gli array: la loro importanza e il loro utilizzo.

>>——Robin——>